AZIENDA OSPEDALIERO – UNIVERSITARIA DI SASSARI

Via Coppino, 26 - 07100 SASSARI – C.F. - P. IVA 02268260904

Deliberazione del Direttore Generale n.195 del 31/03 /2009

Oggetto: Nomina dei Responsabili del trattamento dei dati personali.

L'anno duemilanove, il giorno 31 del mese di marzo, in Sassari, nella sede legale dell'Azienda Ospedaliero-Universitaria

IL DIRETTORE GENERALE
Dott. Renato MURA

VISTO il Decreto Legislativo n. 517 del 21 dicembre 1999;

VISTO il Protocollo d'Intesa sottoscritto dalla Regione Sardegna e dalle Università di Cagliari e di Sassari in data 11 ottobre 2004;

VISTO l'Accordo Regione-Università di Sassari, sottoscritto in data 12.07.2005;

VISTA la Deliberazione della Giunta Regionale della Sardegna n. 17/2 del 27 aprile 2007, con la quale è stata costituita l'Azienda Ospedaliero – Universitaria di Sassari;

VISTO il Decreto n. 100 del 3 settembre 2008 con il quale il Presidente della Regione Autonoma della Sardegna ha nominato il Direttore Generale dell'Azienda Ospedaliero – Universitaria di Sassari nella persona del Dott. Renato Mura;

TENUTO CONTO che il Dott. Renato Mura ha assunto la funzione di Direttore Generale dell'Azienda Ospedaliero - Universitaria di Sassari il giorno 8 settembre 2008, data di stipulazione del relativo contratto;

VISTO il Decreto Legislativo del 30.12.1992, n. 502 "Riordino della disciplina in materia sanitaria";

VISTA la Legge Regionale del 28.07.2006 n. 10, "Tutela della salute e riordino del servizio sanitario della Sardegna";

VISTO il Decreto Legislativo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali", di seguito definito "Codice privacy";

CONSIDERATO che, ai sensi dell'art. 1 del Codice Privacy, chiunque ha diritto alla protezione dei dati personali in conformità alle disposizioni di legge;

CONSIDERATO che il Codice Privacy ha confermato la disciplina in materia di sicurezza dei dati personali già introdotta con la Legge 675/96 ed ha ribadito il dovere di custodire e controllare i dati personali per contenere il più possibile il rischio che siano distrutti, dispersi anche accidentalmente, conoscibili fuori dai casi consentiti o trattati in modo illecito, nonché di introdurre ogni utile dispositivo di protezione legato alle nuove conoscenze tecniche;

VISTO l'art. 33 del Codice Privacy che prevede per i titolari del trattamento l'obbligo di adottare le misure minime di sicurezza volte ad assicurare un livello minimo di protezione dei dati personali;

CONSIDERATO che, in relazione alle c.d. "misure minime" il Codice Privacy agli artt. 34, 35, 36 e nell'allegato B "Disciplinare Tecnico" ha individuato le stesse imponendone l'adozione;

CONSIDERATO che l'art. 4 lett. f) del Codice Privacy individua, fra gli altri, quale Titolare ".....la Pubblica Amministrazione..... cui competono, anche

unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo di sicurezza";

CONSIDERATO che l'azienda Ospedaliero Universitaria di Sassari è "Titolare" del trattamento dei dati da essa trattati con l'ausilio dei mezzi informatici o cartacei ecc.;

VALUTATA l'opportunità, in applicazione degli artt. 29 e 30 del Codice Privacy, che il Titolare, al fine di realizzare gli adempimenti prescritti per l'attuazione puntuale della normativa, individui le figure dei "Responsabili" fornendo indicazione anche per la prossima nomina degli "Incaricati";

VISTO l'art. 4 lettera g) del Codice Privacy che individua quali "Responsabili", fra gli altri, "la persona fisica.....preposta dal Titolare al trattamento dei dati personali";

RILEVATO che, ai sensi dell'art. 29 del Codice Privacy, il "Responsabile" è individuato tra i soggetti che per esperienza , capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza;

VISTO l'art. 4 lettera h) del Codice Privacy che individua quali "Incaricati" "le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile";

RILEVATO che, ai sensi dell'art. 30 del Codice Privacy, le operazioni del trattamento possono esser effettuate solo da Incaricati che operano sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle istruzioni impartite;

RITENUTO opportuno che tutti i Responsabili nominino quali Incaricati le persone fisiche che effettuano trattamenti sotto la diretta autorità del Responsabile;

CONSIDERATO che le operazioni di trattamento sono curate da tutte le unità di personale Sanitario, Tecnico ed Amministrativo, a tempo indeterminato e determinato, ciascuno in relazione alle attività svolte nell'ambito delle Strutture di afferenza;

CONSIDERATO che la designazione, così come prescritto dall'art. 30 del Codice Privacy, dovrà essere effettuata per iscritto e dovrà individuare puntualmente l'ambito del trattamento consentito;

CONSIDERATO comunque, che il Codice Privacy, considera "valida designazione dell'Incaricato" anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima;

CONSIDERATO che, in relazione alla nomina degli Incaricati, il Responsabile potrà procedere secondo due modalità alternative, di cui: a) nella designazione ad personam dei singoli Incaricati, individuando per ciascuno l'ambito dei

trattamenti consentiti; b) nella predisposizione di apposito provvedimento con l'individuazione per ciascuna Struttura delle competenze, degli ambiti dei trattamenti consentiti e dell'indicazione nominativa del personale in servizio presso la stessa Struttura;

ACQUISITI i pareri favorevoli del Direttore Amministrativo e del Direttore Sanitario;

D E L I B E R A

Per i motivi espressi in premessa, che qui si richiamano integralmente:

1) di nominare, ai sensi dell'art. 29 del Codice Privacy, i "Responsabili" del trattamento dei dati:
   a. **Per ciò che attiene la Direzione Generale:**
      - Il Direttore Generale;
   b. **Per ciò che attiene lo Staff:**
      - I Dirigenti ciascuno relativamente ai dati trattati dai rispettivi Servizi per le funzioni ed attività espletate;
   c. **Per ciò che attiene la Direzione Amministrativa:**
      - Il Direttore Amministrativo;
   d. **Per ciò che attiene il Dipartimento Amministrativo e Tecnico:**
      - I Dirigenti ciascuno relativamente ai dati trattati dai rispettivi Servizi per le funzioni ed attività espletate;
   e. **Per ciò che attiene la Direzione Sanitaria:**
      - Il Direttore Sanitario;
   f. **Per ciò che attiene la Direzione Medica di Presidio:**
      - I Dirigenti ciascuno relativamente ai dati trattati dai rispettivi Servizi per le funzioni ed attività espletate;
   g. **Per ciò che attiene il Presidio Ospedaliero:**
      - I Dirigenti Responsabili delle Strutture;
      - I Dirigenti Responsabili delle Unità Operative;
      - I Dirigenti Responsabili dei Programmi ex art5 comma 4 del Decreto Legislativo n. 517 del 21 dicembre 1999;
2) di riservarsi di effettuare ulteriori nomine di "Responsabili" laddove si rendesse necessario, per lo svolgimento delle attività istituzionali, comunicare o delegare a soggetti terzi esterni all'Azienda Ospedaliero Universitaria il trattamento di alcuni dati;
3) di affidare ai "Responsabili" così come sopra individuati, i seguenti compiti:
   I. organizzare gli archivi fisici di competenza, le mansioni dei collaboratori e le operazioni di trattamento dei dati, affinché siano eseguite nel rispetto delle disposizioni di legge, con particolare riferimento all'applicazione delle misure di sicurezza, alle norme relative alle informazioni ed al consenso degli interessati ed all'autorizzazione del Garante;
   II. nominare gli Incaricati, ovvero i collaboratori dipendenti o assimilabili, ai quali vengono affidati i trattamenti dei dati di pertinenza, impartendo loro istruzioni sui modi di operare e sulle misure di sicurezza da applicare durante l'espletamento dei compiti assegnati, consegnando una copia della versione

degli incaricati" compilato dopo l'avvenuta consegna delle Istruzioni agli Incaricati;

III. verificare almeno semestralmente lo stato di applicazione delle direttive del Titolare, nonché il buon funzionamento dei sistemi e la corretta applicazione delle misure di sicurezza;

IV. ove previsto dalla normativa, informare l'Interessato (ovvero il soggetto cui i dati si riferiscono) sulle modalità e finalità del trattamento e raccoglierne il consenso;

V. ove succeda, avvisare immediatamente il Responsabile della Sicurezza Informatica di ogni richiesta, ordine o attività di controllo da parte del Garante o dell'Autorità Giudiziaria, ai sensi degli articoli 152 e da 157 a 160 del Codice Privacy;

VI. quando applicabile, comunicare immediatamente al Responsabile della Sicurezza Informatica gli eventuali nuovi trattamenti da intraprendere nel settore di competenza, provvedendo alle necessarie formalità di Legge;

VII. dare piena collaborazione al Responsabile della Sicurezza Informatica per rispondere alle istanze avanzate dall'Interessato o da un suo Incaricato, o ad evadere tempestivamente le richieste di informazioni da parte dell'Autorità Garante e dare immediata esecuzione delle indicazioni che perverranno dalla medesima;

VIII. distruggere i dati personali in caso di cessazione del trattamento degli stessi nei termini previsti dalla Legge, provvedendo alle necessarie formalità;

IX. utilizzare le versioni correnti di tutti i documenti consolidati dal Titolare con la collaborazione di tutti i Responsabili, che saranno pubblicati e resi disponibili in forma cartacea e/o elettronica dal Responsabile della Sicurezza Informatica secondo le disposizioni ricevute;

4) di approvare lo schema di nomina dei "Responsabili" allegato alla presente deliberazione per farne parte integrante e sostanziale (allegato n. 1);

5) di approvare lo schema di nomina degli "Incaricati" allegato alla presente deliberazione per farne parte integrante e sostanziale (allegato n. 2);

6) di approvare le linee guida per i Responsabili "Le misure di sicurezza per la tutela della privacy dei dati personali e sensibili" allegate alla presente deliberazione per farne parte integrante e sostanziale (allegato n. 3);

7) di approvare le "Misure di sicurezza da applicare nei trattamenti di dati con strumenti elettronici" allegate alla presente deliberazione per farne parte integrante e sostanziale (allegato n. 4);

8) di approvare lo schema del Registro di designazione degli "Incaricati" allegato alla presente deliberazione per farne parte integrante e sostanziale (allegato n. 5);

9) di incaricare i servizi competenti dell'esecuzione del presente provvedimento.

IL DIRETTORE GENERALE
(Dott. Renato MURA)

IL DIRETTORE AMMINISTRATIVO
(Dott. Giuseppe PINTOR)

IL DIRETTORE SANITARIO
(Dott. Nicola LICHERI)

Responsabile Struttura Proponente nel rispetto del budget di spesa annua assegnata. Nome Struttura _____ Sigla Responsabile _____ Estensore _____	Responsabile del Bilancio in ordine alla relativa copertura finanziaria. _____

La presente deliberazione è in pubblicazione all'Albo Pretorio di questa Azienda Ospedaliero - Universitaria di Sassari dal 31/03/09 per la durata di quindici giorni.

Allegato n. 1

AZIENDA OSPEDALIERO UNIVERSITARIA DI SASSARI

ATTO DI NOMINA DEL RESPONSABILE, AI SENSI E PER GLI EFFETTI DEL D.LGS. 30 GIUGNO 2003 N.196

AL DOTT./SIG.....

OGGETTO: RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL' ART. 29 D.LGS 196/03

IL DIRETTORE GENERALE DOTT. RENATO MURA, IN QUALITÀ DI TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

NOMINA

IL PROF./DOTT./ DELLA STRUTTURA.....,

RESPONSABILE DEL TRATTATMENTO DEI DATI TRATTATI DAL

IL RESPONSABILE HA IL POTERE DOVERE DI COMPIERE TUTTO QUANTO SI RENDERÀ NECESSARIO AI FINI DEL RISPETTO E DELLA CORRETTA APPLICAZIONE DEL T.U. SULLA PRIVACY. IL RESPONSABILE È TENUTO A:

I. organizzare gli archivi fisici di competenza, le mansioni dei collaboratori e le operazioni di trattamento dei dati, affinché siano eseguite nel rispetto delle disposizioni di legge, con particolare riferimento all' applicazione delle misure di sicurezza, alle norme relative alle informazioni ed al consenso degli interessati ed all'autorizzazione del Garante;

II. nominare gli Incaricati, ovvero i collaboratori dipendenti o assimilabili, ai quali vengono affidati i trattamenti dei dati di pertinenza, impartendo loro istruzioni sui modi di operare e sulle misure di sicurezza da applicare durante l'espletamento dei compiti assegnati, consegnando una copia della versione corrente del documento "Misure di sicurezza da applicare nei trattamenti di dati con strumenti elettronici" e dando riscontro al Responsabile della Sicurezza Informatica, inviandogli il modulo "Registro degli incaricati" compilato dopo l'avvenuta consegna delle Istruzioni agli Incaricati;

III. verificare almeno semestralmente lo stato di applicazione delle direttive del Titolare, nonché il buon funzionamento dei sistemi e la corretta applicazione delle misure di sicurezza;

IV. ove previsto dalla normativa, informare l'interessato (ovvero il soggetto cui i dati si riferiscono) sulle modalità e finalità del trattamento e raccoglierne il consenso;

V. ove succeda, avvisare immediatamente il Responsabile della Sicurezza Informatica di ogni richiesta, ordine o attività di controllo da parte del Garante o dell'Autorità Giudiziaria, ai sensi degli articoli 152 e da 157 a 160 del Codice Privacy;

VI. quando applicabile, comunicare immediatamente al Responsabile della

Sicurezza Informatica gli eventuali nuovi trattamenti da intraprendere nel settore di competenza, provvedendo alle necessarie formalità di Legge;

VII. dare piena collaborazione al Responsabile della Sicurezza per rispondere alle istanze avanzate dall'Interessato o da un suo Incaricato, o ad evadere tempestivamente le richieste di informazioni da parte dell'Autorità Garante e dare immediata esecuzione delle indicazioni che perverranno dalla medesima;

VIII. distruggere i dati personali in caso di cessazione del trattamento degli stessi nei termini previsti dalla Legge, provvedendo alle necessarie formalità;

IX. utilizzare le versioni correnti di tutti i documenti consolidati dal Titolare con la collaborazione di tutti i Responsabili, che saranno pubblicati e resi disponibili in forma cartacea e/o elettronica dal Responsabile della Sicurezza Informatica, secondo le disposizioni ricevute.

IL DIRETTORE GENERALE
DOTT. RENATO MURA

Allegato n. 2

AZIENDA OSPEDALIERO UNIVERSITARIA DI SASSARI

ATTO DI NOMINA DELL'INCARICATO, AI SENSI E PER GLI EFFETTI DEL D.LGS. 30 GIUGNO 2003, N. 196

AL DOTT./SIG.....

OGGETTO: INCARICATO AL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL' ART. 30 D.LGS 196/03

IL SOTTOSCRITTO PROF./DOTT.....,
IN QUALITÀ DI RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI DELLA STRUTTURA

NOMINATO DAL TITOLARE QUALE RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI PRESSO LA SOPRA INDICATA

STRUTTURA DELL'AZIENDA OSPEDALIERO UNIVERSITARIA DI SASSARI

INCARICA

il Prof./Dott./Sig....., /C.F. ..... IN SERVIZIO

PRESSO LA STRUTTURA....., DI EFFETTUARE I TRATTAMENTI DEI DATI PERSONALI, ANCHE SENSIBILI E

GIUDIZIARI, CON ACCESSO AI DATI LA CUI CONOSCENZA SIA STRETTAMENTE NECESSARIA PER ADEMPIERE AI COMPITI

ASSEGNATI:

BANCA DATI/ARCHIVIO CARTACEO	Trattamenti[1]	Compiti[2]	Natura dei dati[3]		FIRMA INCARICATI	Revoca[4]
			S	G		

LA S.V. DOVRÀ ATTENERSI AI CRITERI PREVISTI DALLA NORMATIVA VIGENTE SULLA TUTELA DEI DATI PERSONALI E SULLE MISURE DI SICUREZZA RELATIVE, ANCHE CON RIFERIMENTO ALLE NORME ED ALLE MODALITÀ TECNICHE ADOTTATE DA QUESTA AZIENDA.

1 Indicare i trattamenti ai quali l'incaricato è abilitato:
CRE(CREAZIONE); CREA ED ORGANIZZA L'ARCHIVIO, RACCOGLIE, REGISTRA ED INSERISCE NUOVI DATI
MOD(MODIFICA); MODIFICA, ESTRAE, ELABORA E CANCELLA (IN SENSO LOGICO, NON FISICO) I DATI
LET(LETTURA); SELEZIONA, RAFFRONTA E CONSULTA I DATI
COM(COMUNICAZIONE / DIFFUSIONE); DIFFONDE E COMUNICA L'INFORMAZIONE
ARC(ARCHIVIAZIONE); ARCHIVIA I DATI
ELA(ELABORAZIONE/ CONSERVAZIONE); ELABORA E CONSERVA I DATI IN FORMATO DIGITALE
COMPLETO; ABILITATO A TUTTI I TRATTAMENTI PREVISTI
2 Indicare i compiti lavorativi da svolgere
3 Indicare se la banca dati/archivio cartaceo a cui è consentito l'accesso contiene dati sensibili o giudiziari, apponendo una X nell'apposita casella.
4 Inserire la data della revoca in corrispondenza del nominativo dell'incaricato al quale viene revocato l'incarico.

Al riguardo, la S.V. si impegna ad effettuare il trattamento dei dati di competenza osservando le istruzioni riportate nelle Istruzioni per il trattamento dei dati allegate alla presente ed in ogni altra indicazione che potrà essere fornita dal Responsabile del trattamento.

Lì, _____

Il Responsabile del trattamento

_____

L'incaricato

_____

Allegato n. 5

Registro Designazione Incaricati

Struttura:		Responsabile:	

Designazione, ai sensi dell'art. 30, 2°comma, d.lgs.n.196/2003, degli incaricati del trattamento di dati personali effettuati nell'ambito della Struttura.

Nominativo	Unità Appartenenza	Mansione o ambito di trattamento	Data	Firma Incaricato

Nota: barrare le righe non utilizzate

Si dichiara che le persone sopra elencate sono nominate INCARICATI DEI TRATTAMENTI nell'ambito di competenza. Ad ciascuno di loro è stato consegnato il documento – Istruzioni per la Sicurezza dei Dati - "Misure di sicurezza da applicare nei trattamenti di dati con strumenti elettronici".

Data:	**Firma Responsabile**

AOU

Azienda Ospedaliero Universitaria di Sassari

LINEE GUIDA PER I RESPONSABILI

DEL TRATTAMENTO DEI DATI PERSONALI

Le misure di sicurezza per la tutela della privacy dei dati personali e sensibili

Documento	AOU-DPS-LG/1
Edizione	31/03/2009

Premessa

L'**autorità Garante della Privacy**, istituita nel 1996, si propone di tutelare il diritto alla privacy di tutti, sia che si tratti di persone fisiche ovvero di persone giuridiche, enti o associazioni. Vengono quindi focalizzati tutti i processi aziendali che interessano dati personali, entrando nel merito delle finalità e della liceità dei "trattamenti" che vengono effettuati.

In questo contesto l'Azienda Ospedaliero Universitaria di Sassari, in qualità di titolare dei trattamenti dei dati necessari per l'espletamento della propria missione, dopo aver provveduto agli adempimenti previsti dalla Legge, intende sensibilizzare tutto il personale alle misure di sicurezza per la tutela dei dati e della Privacy.

Queste "linee guida" sono in particolare destinate ai Responsabili di strutture complesse, semplici e di Programmi ex art. ex art 5 comma 4 del Decreto Legislativo n. 517 del 21 dicembre 1999, per ricordare a ciascuno l'osservanza delle direttive aziendali in materia di sicurezza in Azienda.

Le "linee guida" sono state strutturate nei seguenti capitoli:

- Il Decreto Legislativo 196/03 in sintesi – per illustrare gli aspetti fondamentali del testo unico e fornire utili riferimenti per eventuali approfondimenti sulla materia
- L'organizzazione per la sicurezza – per illustrare la ripartizione delle Responsabilità e dei compiti per la tutela dei dati personali nel contesto operativo dell'Azienda Ospedaliero Universitaria di Sassari.
- Le misure di sicurezza – per fornire indicazioni sulle misure di sicurezza adottate in azienda, alle quali tutti devono attenersi
- L'affidamento di dati personali all'esterno – per illustrare i criteri applicati per garantire l'adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all'esterno
- Il controllo generale sullo stato della sicurezza -- le procedure previste per il controllo sullo stato della sicurezza

1 Il Decreto Legislativo 196/03 in sintesi

Il "Testo Unico sulla Privacy" (D. lgs.196/03: "Codice") entrato in vigore il primo gennaio 2004, riprende ed integra la normativa introdotta dalla Legge 675/96 e dal DPR.318/99, prevedendo l'obbligo di garantire la sicurezza, l'integrità e la disponibilità dei dati personali.

Citiamo per chiarezza alcuni passaggi significativi del codice:

Diritto alla protezione dei dati personali: art. 1 del TU

"Chiunque ha diritto alla protezione dei dati personali che lo riguardano."

Come si nota, l'art.1 introduce nell'ordinamento il "diritto alla protezione dei dati personali", diritto fondamentale della persona, autonomo rispetto al più generale diritto alla riservatezza: un diritto che tiene conto delle molteplici prerogative legate al trattamento dei dati personali, anche oltre quelle attinenti al riserbo e alla tutela della vita privata.

In tal modo il legislatore italiano si adegua al quadro normativo comunitario che, nella Carta dei diritti del cittadino europeo, garantisce già tale diritto fondamentale (art. 8) che si accinge ad assumere una connotazione ancora più solenne nel quadro dei lavori della Convenzione europea.

Principio di necessità nel trattamento dei dati: art. 3 del TU

"I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità."

L'art. 3 introduce il "principio di necessità" nel trattamento dei dati personali, in base al quale, sin dalla loro configurazione, i sistemi informativi ed i software devono essere predisposti in modo da assicurare che i dati personali o identificativi siano utilizzati solo se indispensabili per il raggiungimento delle finalità consentite, e non anche quando i medesimi obiettivi possano essere raggiunti mediante l'uso di dati anonimi o che comunque consentano una più circoscritta identificazione degli interessati.

Il principio introdotto integra e completa, con riferimento alla configurazione stessa dell'ambiente in cui i dati sono trattati, il principio di pertinenza e non eccedenza dei dati trattati già operante in relazione al trattamento dei medesimi dati (art. 11, già art. 9, l. n. 675/1996).

Si tratta di una regola di ordine generale in specie per i sistemi e i programmi che verranno d'ora in poi predisposti.

Con il testo unico, che assume le caratteristiche di un vero e proprio "codice privacy e sicurezza", il legislatore ha provveduto a coordinare le norme sinora vigenti in materia, apportando inoltre numerose integrazioni e modificazioni, anche per assicurare una migliore e più chiara attuazione della normativa.

1.1 La struttura del TU

Il nuovo **codice** si compone di tre parti, che contengono, rispettivamente:

1. le **disposizioni generali** (articoli da 1 a 45), riguardanti le regole *sostanziali* della disciplina del trattamento dei dati personali, applicabili a tutti i trattamenti, nonché le regole specifiche che si devono osservare per i trattamenti effettuati da soggetti *pubblici* e quelle che trovano applicazione per i trattamenti effettuati da soggetti *privati* e da *enti pubblici economici;*
2. le disposizioni particolari, che si applicano per specifici trattamenti (articoli da 46 a 140), ad integrazione o eccezione alle disposizioni generali, contenute nella Prima parte;

3. le disposizioni relative alle **azioni di tutela** dell'interessato e al **sistema sanzionatorio** (articoli da 141 a 172), cui si aggiungono le norme di modifica, finali e di carattere transitorio (articoli da 173 a 186).

Il codice è completato da **tre allegati**, le cui disposizioni si devono quindi intendere come parte integrante dello stesso, contenenti quanto segue:

- i **codici di deontologia** (*allegato A*), a partire dai tre che risultano ad oggi approvati (riguardanti rispettivamente l'attività giornalistica, gli scopi storici e gli scopi statistici nell'ambito del SISTAN - Sistema statistico nazionale), ai quali andranno ad aggiungersi quelli di futura approvazione;
- il **disciplinare tecnico in materia di misure minime di sicurezza** (*allegato B*), il quale potrà essere adeguato all'evoluzione del settore, in modo flessibile, con decreti ministeriali non regolamentari;
- l'elenco dei trattamenti non occasionali effettuati in **ambito giudiziario o per fini di polizia** (*allegato C*), che in sede di prima applicazione della normativa dovranno essere individuati, entro il 30 giugno 2004, dai Ministeri competenti.

Come utile riferimento, in allegato è riprodotto l'indice completo del decreto legislativo sopra citato, dal quale si può apprezzare come il Garante abbia voluto strutturare questo Testo Unico.

1.2 Definizioni

Citando l'art 4 del TU:

a) **"trattamento"**, qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

b) **"dato personale"**, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

c) **"dati identificativi"**, i dati personali che permettono l'identificazione diretta dell'interessato;

d) **"dati sensibili"**, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

e) **"dati giudiziari"**, i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

f) **"Titolare"**, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

g) **"Responsabile"**, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h) **"Incaricati"**, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal Responsabile;

i) **"interessato"**, la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

l) **"comunicazione"**, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal Responsabile e dagli Incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

m) **"diffusione"**, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

n) **"dato anonimo",** il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

o) **"blocco",** la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

p) **"banca di dati",** qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

q) **"Garante",** l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

E' opportuno evidenziare che il nuovo codice ha ufficializzato i seguenti punti, che si erano già affermati nella pratica e nelle interpretazioni fornite dal Garante:

-- tra le decisioni che competono al titolare vi sono anche quelle in merito alla delega operativa ai Responsabili e agli strumenti utilizzati per trattare i dati personali;

-- il ruolo di Incaricato del trattamento può essere rivestito solo da una persona fisica; quindi non da società ed enti.

1.3 Due parole sulla natura dei dati personali

Dalla definizione di partenza si desume innanzitutto che il dato personale è una informazione su un soggetto, sia esso una persona fisica, una persona giuridica, un ente od una associazione: ciò porta ad escludere dalla definizione la semplice combinazione di nome, cognome, luogo e data di nascita di una persona.

La frase: "Mario Rossi, nato il 25 febbraio 1958 a Milano" non è un dato sensibile, in quanto prende oggettivamente atto dell'esistenza dell'individuo Mario Rossi, senza fornire alcuna informazione in merito alla vita del suddetto. Lo stesso può dirsi per la semplice denominazione di una società.

Ma ciò è sempre vero? Per i Mario Rossi di tutto il mondo sicuramente sì. E per "Abramo Levi, nato a Tel Aviv il 12 febbraio 1958" ?

In questo caso la semplice combinazione di elementi anagrafici "di base" può svelare una precisa informazione in merito alla religione ed al gruppo etnico di appartenenza del soggetto: informazione che, per inciso, è definita dalla legge come "sensibile", e quindi meritevole di particolare tutela.

Questo esempio induce a formulare una prima riflessione: in taluni casi il confine tra ciò che è "dato sensibile" e ciò che non lo è sfuma, e la risposta in merito dipende in ultima analisi dalle **concrete finalità** perseguite da chi possiede e tratta i dati.

Se, ad esempio, il fine fosse semplicemente di annotare i dati anagrafici di Abramo Levi per fargli gli auguri di compleanno, non si sarebbe nel campo dei dati sensibili. Se invece tale dato fosse utilizzato da un commerciante di oggettistica religiosa, l'informazione assurgerebbe al rango di dato sensibile, in quanto in tale contesto non rileverebbero i dati anagrafici dell'individuo, ma la sua appartenenza ad una religione.

Nella frase *Abramo Levi è di religione ebraica* il vero dato sensibile è cioè costituito dalla appartenenza del soggetto ad una precisa categoria di individui (le persone di religione ebraica). La combinazione di nome e cognome (Abramo Levi) diventa rilevante, solo in quanto essa viene usata come strumento per riferire una situazione o una qualità ad un determinato individuo.

Tornando a Mario Rossi, Mario Rossi, residente in Piazza del Popolo 2, Firenze è invece certamente un dato personale, in quanto fornisce l'informazione su dove il suddetto individuo risieda.

Così come è un dato personale Sigma Spa, con sede in via dell'Industria 2, Milano, poiché la legge estende il proprio ambito di applicazione ai dati che concernono persone giuridiche, enti ed associazioni, con la sola esclusione degli Organi che costituiscono la Pubblica Amministrazione.

La legge trova applicazione anche per i dati che riguardano soggetti non residenti: sono quindi ad esempio considerati dati personali, e come tali vanno trattati, quelli di John Smith di New York, piuttosto che della Ford Inc. di Detroit.

In una decisione presa nel 1999, il Garante ha precisato che l'espressione qualunque informazione vuole evidentemente attribuire alla definizione di dato personale la massima ampiezza, comprendendo anche ogni notizia, informazione o elemento che abbia un'efficacia informativa tale, da fornire un contributo aggiuntivo di conoscenza rispetto ad un soggetto identificato od identificabile.

E ciò in riferimento sia ad informazioni oggettivamente caratterizzate, suscettibili di una verifica e di un sindacato obiettivo (es. indirizzo e numero di telefono; dato relativo alle ore di servizio prestate da un dipendente, in un determinato arco temporale), che a descrizioni, giudizi, analisi o ricostruzioni di profili personali, che danno origine a stime ed opinioni di natura soggettiva, finalizzate anche ad una valutazione complessiva del soggetto interessato.

Esempi di valutazioni di carattere soggettivo, che sono a tutti gli effetti considerate dati personali, sono:

- le valutazioni, effettuate da una banca, sul grado di affidabilità di un soggetto che richiede un finanziamento, nonché le eventuali motivazioni anche "interne" che sono alla base del rifiuto di concederlo;
- una diagnosi medica, anche per la parte che comprende elementi valutativi o di prognosi di tipo discrezionale;
- le note di qualifica, cioè le valutazioni che contribuiscono a formare il giudizio annuale sul rendimento di un dipendente.
-

Si sono citate le tipologie di dati che, scorrendo i ricorsi decisi dal Garante, più di frequente sono oggetto di contenzioso, che si conclude inevitabilmente con la condanna di chi effettua il trattamento, per avere negato l'accesso ai soggetti cui tali dati si riferiscono.

Con queste considerazioni in mente, è opportuno quindi pensare che qualunque dato aziendale merita attenzione da parte di chi lo tratta, non solo per la sua possibile valenza come dato di natura personale, ma anche per l'importanza che esso riveste per l'azienda stessa.

1.4 L'uso degli strumenti informatici

Avendo introdotto un netto distinguo tra il trattamento effettuato con e senza strumenti elettronici, il legislatore ha ritenuto opportuno scendere nel dettaglio delle modalità di accesso alle informazioni e il trattamento avviene con l'ausilio di strumenti informatici.

L'adozione di adeguate misure di sicurezza è resa obbligatoria per tutti i soggetti che trattano dati personali, con particolare attenzione per quelli sensibili e giudiziari.

Con il DL 196/2003 viene anche esplicitato il quadro delle **misure minime di sicurezza** (art. 33 T.U.), che configurano il livello minimo di protezione richiesto dalla normativa per contrastare i rischi di perdita, di alterazione, di distruzione e di uso improprio dei dati.

Egli ha quindi utilizzato i termini "autenticazione/autorizzazione" per regolamentare l'accesso alle informazioni con l'ausilio di strumenti informatici.

Questo comporta che l'utente (titolare, Responsabile od Incaricato) autorizzato al trattamento debba possedere quelle che sono indicate come "credenziali di autenticazione"

- un **nome utente** ed una **password** di accesso ai sistemi; tali informazioni devono essere note solo ed esclusivamente all'utente autorizzato all'accesso ai dati;
- **dispositivo di autenticazione**; è previsto l'impiego di tecnologie che utilizzano dispositivi fisici per l'autenticazione ai sistemi (badge, smart cards, etc.)
- caratteristiche **biometriche**, ovvero utilizzo di dispositivi di rilevazione biometrica (impronta digitale, iride, etc) che possono essere associati ad una password;

Citiamo per maggiore chiarezza altri estratti significativi del decreto legislativo:

Obblighi di sicurezza : art. 31 del T.U.

"I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati ed alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo,

mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".

Misure minime di sicurezza : art. 33 del T.U.

"Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

L'adozione delle Misure Minime di Sicurezza è obbligatoria per tutti coloro che effettuano trattamenti di dati personali."

Sanzioni : art. 169 del T.U.

"Chiunque, essendovi tenuto, omette di adottare il misure minime previste dall'art. 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro."

1.5 L'organizzazione per la sicurezza

L'Azienda Ospedaliero Universitaria di Sassari, nella consapevolezza che un sistema complesso quale la sicurezza può funzionare solo se i suoi meccanismi sono formalizzati e verificabili, nonché posti in essere da personale adeguatamente formato e motivato, per l'applicazione e la gestione della normativa sulla privacy, ha provveduto ad adottare la seguente organizzazione per la sicurezza.

1.6 Titolare del Trattamento

Ai sensi dell'art.4, lett. f) del Codice in materia di protezione dei dati personali, il Titolare dei trattamenti è l'AOU di Sassari nella persona del Direttore Generale.

Per Titolare si intende la persona fisica, persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, in piena autonomia, le decisioni in ordine alle finalità e alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Il titolare, in quanto tale, è Responsabile dell'analisi e della valutazione dei rischi che incombono sui dati e dell'applicazione delle misure minime di sicurezza.

Il Titolare ha a facoltà di nominare uno o più Responsabili che possono essere interni o esterni, impartendo loro le direttive alle quali devono attenersi nella gestione e trattamento dei dati personali che gli sono stati affidati;

Il Titolare verificherà periodicamente che le istruzioni e le norme di legge in tema di privacy vengano correttamente applicate dai Responsabili.

1.7 Responsabili del Trattamento

Il Titolare, nella persona del Direttore Generale dell'Azienda Ospedaliero Universitaria di Sassari, ha nominato Responsabili dei Trattamenti tutti i Dirigenti di Struttura , i Dirigenti delle Unità Operative , li Dirigenti Responsabili dei programmi ex art. 3 comma 4 del D. Lgs. N. 517/99 e i Dirigenti Responsabili dei Servizi Amministrativi dell'Azienda.

I compiti dei Responsabili i sono i seguenti:

- nominare gli Incaricati ovvero le persone fisiche ai quali, all'interno della propria struttura, è affidato il compito di trattare i dati personali;
- impartire istruzioni precise e dettagliate agli Incaricati;
- controllare le attività degli Incaricati, procedendo a verifiche periodiche, in conformità alle direttive dei Titolari/Contitolari;
- informare l'interessato (ovvero il soggetto cui i dati si riferiscono) sulle modalità e finalità del trattamento e raccoglierne il consenso, ove previsto dalla normativa;
- rispondere alle istanze avanzate dall'interessato o da un suo Incaricato.

1.8 Responsabile per la Sicurezza Informatica

Il Titolare, nella persona del Direttore Generale dell'Azienda Ospedaliera Universitaria di Sassari, *nomina il* Responsabile per la Sicurezza Informatica.

Al Responsabile per la Sicurezza Informatica, viene affidata la pianificazione, l'organizzazione, l'attuazione (anche mediante l'eventuale ricorso a qualificati soggetti esterni) delle infrastrutture informatiche centralizzate, delle procedure e di tutte le iniziative aziendali ritenute necessarie ed opportune per progressivamente migliorare le misure di sicurezza informatica indispensabili a garantire la sicurezza dei trattamenti effettuati con strumenti elettronici.

In particolare, al Responsabile per la Sicurezza Informatica sono assegnati i compiti di:

- raccogliere le informazioni da ciascun Responsabile per elaborare la mappa dei trattamenti di dati personali, effettuati dall'Azienda, combinando la tipologia dei dati trattati con gli strumenti che vengono impiegati per il trattamento;
- sulla base di tale mappa, effettuare una analisi dei rischi che gravano sui dati informatizzati e sugli strumenti, identificando di conseguenza gli elementi da proteggere e le minacce cui essi sono sottoposti;
- sulla base dell'analisi dei rischi, definire i requisiti di sicurezza da adottare, per proteggere il complesso degli archivi elettronici di dati personali, delle procedure e dei sistemi informativi esistenti, osservando quanto prescritto dal Dlgs 196/2003 e dal relativo disciplinare tecnico allegato sub B);
- progettare, implementare e progressivamente migliorare il sistema di sicurezza dei sistemi informativi e dell'infrastruttura informatica aziendale, in base ai requisiti definiti nel punto precedente, mediante l'adozione delle opportune misure centralizzate e decentrate:
  - organizzative, che si sostanziano nella definizione di una serie di norme e procedure, miranti a regolamentare l'aspetto organizzativo del processo di sicurezza dei trattamenti effettuati con strumenti elettronici;
  - fisiche, il cui scopo è di proteggere le aree, le apparecchiature informatiche e i dati da eventi di natura accidentale e da intrusioni di personale non autorizzato o di terzi;
  - logiche, il cui campo di applicazione riguarda la protezione delle informazioni, con particolare riferimento a quelle gestite con i sistemi informativi (dati, applicazioni, sistemi e reti);
- pianificare e curare l'attuazione, anche a cura di soggetti specializzati esterni, degli interventi di monitoraggio della sicurezza e dei test di penetrazione e predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno annuale, dell'efficacia delle misure di sicurezza adottate;
- assicurarsi che siano adeguatamente predisposti e mantenuti in efficienza sistemi e procedure di ripristino dei dati, nel caso in cui essi siano colpiti da eventi che possano danneggiarli o addirittura distruggerli, con l'obiettivo di renderli nuovamente disponibili entro un lasso di tempo ragionevole, avendo riguardo all'efficienza dell'organizzazione;
- garantire che sia effettuata la manutenzione del sistema di sicurezza informatica, per assicurarne la costante efficienza e disponibilità, nonché procedere al suo aggiornamento periodico, per renderlo sempre adeguato alle nuove minacce;
- programmare e curare la realizzazione del piano di formazione del personale dell'organizzazione, in tema di sicurezza, finalizzato anche alla emanazione ed al rispetto di procedure interne inerenti la sicurezza (regolamentazione degli accessi fisici e logici agli archivi ed ai sistemi informativi, norme operative di utilizzo e gestione dei sistemi, gestione delle password, ecc.....);

- verificare che i soggetti esterni, cui l'Azienda dovesse affidare il trattamento di dati personali informatizzati, adottino misure di sicurezza conformi a quelle minime, previste dagli articoli da 33 a 35 D. lgs.196/2003 e dal relativo disciplinare tecnico, allegato sub B) al D. lgs. 196/2003 stesso;
- procedere alla redazione e/o all'aggiornamento annuale (eventualmente avvalendosi di qualificati soggetti specializzati esterni), entro il 31 marzo di ogni anno, del Documento Programmatico sulla Sicurezza, curando il previsto *iter* per l'approvazione.

Il Responsabile per la Sicurezza Informatica ha il compito di definire e consolidare progressivamente le "linee guida" e le istruzioni generali in merito ai seguenti punti, aventi specifica attinenza con la sicurezza nell'uso degli strumenti informatici:

- procedure da seguire per la classificazione dei dati, al fine di distinguere quelli sensibili e giudiziari, per garantire la sicurezza dei quali occorrono maggiori cautele, rispetto a quanto è previsto per i dati di natura comune;
- modalità per elaborare e custodire le password, necessarie per accedere agli elaboratori elettronici ed ai dati in essi contenuti, nonché per fornirne una copia al preposto alla custodia delle parole chiave;
- procedure da seguire per non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro;
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi;
- procedure per il salvataggio dei dati e verifica della loro ripristinabilità;
- modalità di custodia ed utilizzo dei supporti rimuovibili, contenenti dati personali.

Ai soggetti incaricati della gestione e manutenzione del sistema informativo, siano essi interni o esterni all'Azienda, viene prescritto di non effettuare alcun trattamento, sui dati personali contenuti negli strumenti elettronici, fatta unicamente eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.

1.9 Incaricati

Il Titolare, nella persona del Direttore Generale dell'Azienda Ospedaliero Universitaria di Sassari, ha assegnato ai Responsabili la delega per la designazione obbligatoria degli Incaricati, avvalendosi della modalità semplificata introdotta dall'art. 30, comma 2, del Codice per individuare l'ambito di trattamento consentito agli addetti alle strutture e alle unità organizzative di pertinenza.

L'Incaricato assume, in ordine al trattamento, funzioni operative in aderenza a specifiche istruzioni ricevute dal Titolare o dal suo Responsabile.

La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito; si considera tale, secondo la normativa anche la documentata preposizione della persona fisica ad una unità organizzativa ove viene individuato l'ambito del trattamento consentito agli addetti all'unità medesima.

Le operazioni di trattamento di dati personali possono essere effettuate solo dagli Incaricati che operano sotto la diretta autorità del Titolare o dei loro Responsabili.

Oltre alle istruzioni generali, su come devono essere trattati i dati personali, agli Incaricati vengono fornite esplicite istruzioni in merito ai seguenti punti, aventi specifica attinenza con la sicurezza:

- procedure da seguire per la classificazione dei dati, al fine di distinguere quelli sensibili e giudiziari, per garantire la sicurezza dei quali occorrono maggiori cautele, rispetto a quanto è previsto per i dati di natura comune;
- modalità di reperimento dei documenti, contenenti dati personali, e modalità da osservare per la custodia degli stessi e la loro archiviazione, al termine dello svolgimento del lavoro per il quale è stato necessario utilizzare i documenti;

- modalità per elaborare e custodire le password, necessarie per accedere agli elaboratori elettronici ed ai dati in essi contenuti, nonché per fornirne una copia al preposto alla custodia delle parole chiave;
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro;
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi;
- procedure per il salvataggio dei dati;
- modalità di custodia ed utilizzo dei supporti rimuovibili, contenenti dati personali;
- dovere di aggiornarsi, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

Si tenga presente che tutto il personale sanitario, amministrativo e tecnico dell'Azienda Ospedaliero Universitaria che in qualche misura svolge attività che implicano il trattamento di dati personali, con particolare attenzione per quelli sensibili e giudiziari, dovrà essere designato quale Incaricato dei trattamenti di competenza.

2 Le misure di sicurezza

Non c'è privacy senza sicurezza

La questione sicurezza non riguarda infatti i soli dati trattati elettronicamente. Tale aspetto è oggi certo di primaria importanza, ma non è l'unico. La sicurezza si ottiene anche con l'uso delle tradizionali chiavi e con la vigilanza delle strutture esterne e dei locali.

Ma non basta ancora, perché si è finora parlato delle ***misure di sicurezza fisiche***, accennato a quelle ***logiche legate all'informatica***, ma non si deve dimenticare l'aspetto più importante: le ***misure organizzative***, il cui fine è di fare in modo che l'intera struttura adotti comportamenti conformi ai principi della sicurezza e, più in generale, della privacy.

A nulla serve essere estremamente scrupolosi nel trattamento dei dati, inviando informative, acquisendo consensi ed autorizzazioni, aggiornandoli con maniacale puntualità, se si lasciano poi i supporti contenenti i dati incustoditi sulla scrivania, alla mercé di chiunque possa entrare nell'ufficio.

2.1 L'insieme delle misure di sicurezza

La sicurezza non deve essere intesa solo come protezione da eventi negativi, accidentali o intenzionali, ma anche come limitazione degli effetti causati dall'eventuale verificarsi di tali eventi di:

- **distruzione o perdita, anche accidentale, dei dati**: ossia si deve impedire che dati, informazioni e risorse siano resi irreperibili da persone, mediante processi non autorizzati, o da eventi accidentali. Nel mondo informatico si ricorre al concetto di ***disponibilità del dato,*** in tale ambito assume inoltre una particolare valenza il requisito della ***integrità del dato***, che deve essere quello originario o legittimamente modificato, in relazione alla relativa facilità di procedere fraudolentemente a modifiche senza lasciare indizi;
- **accesso non autorizzato ai dati**: nel mondo fisico è immediato pensare ad estranei, che nella notte si introducono in un'azienda per rubare dei dati o farne delle copie, piuttosto che a personale dell'azienda stessa che viola determinati archivi durante l'orario di lavoro. Nel mondo informatico si parla di ***confidenzialità*** o ***riservatezza,*** con ciò intendendosi che un determinato dato deve essere accessibile solo a chi è autorizzato: si dovrà quindi fare in modo che il personale non possa consultare files che non lo riguardano; che estranei non possano accedere abusivamente al sistema informativo; che durante la trasmissione di dati da un computer ad un altro, dei malintenzionati non intercettino i messaggi per violare le informazioni in essi contenuti. Correlato a tali aspetti vi è il requisito della ***autenticità*** dei dati, che concerne la garanzia e certificazione della loro provenienza;
- trattamento non consentito o non conforme alle finalità della raccolta.

Si noti che la legge parla realisticamente di "riduzione al minimo", non di eliminazione dei rischi, nella consapevolezza che il raggiungimento di tale assoluto obiettivo è di fatto quasi impossibile, di fronte a tentativi reiterati e sofisticati di violazione della sicurezza delle informazioni da parte di soggetti malintenzionati .

Un'importante osservazione concerne il fatto che viene preteso un *diverso grado di diligenza*, che varia in funzione della *natura dei dati* e delle *specifiche caratteristiche* del trattamento.

E' ovvio che, per custodire un banale elenco di dati anagrafici di taluni abitanti di una città, non è necessario l'uso di una cassaforte con dieci combinazioni, né l'adozione di altro accorgimento, che non sia di riporre l'elenco nel cassetto dotato della solita serratura.

Chi custodisce un elenco contenente nomi cognomi ed indirizzi di persone affette da gravi problemi di salute, con dovizia descritti, è invece tenuto ad adottare più efficaci accorgimenti, a salvaguardia della sicurezza.

L'insieme delle misure di sicurezza viene quindi concettualmente suddiviso in tre sottoinsiemi, distinguendo le ***misure***:

- ***organizzative***, che si sostanziano nella definizione di una serie di norme e procedure, miranti a regolamentare l'aspetto organizzativo del processo di sicurezza;
- ***fisiche***, il cui scopo è di proteggere le aree, le apparecchiature, i dati e le persone da eventi di natura accidentale (es. incendi) e da intrusioni, di personale non autorizzato o di terzi;
- ***logiche***, il cui campo di applicazione riguarda la protezione delle informazioni, con particolare riferimento a quelle gestite con i sistemi informativi (dati, applicazioni, sistemi e reti), sia in relazione al loro corretto utilizzo, che in relazione alla loro gestione e manutenzione nel tempo.

2.2 Cosa richiede il Codice

L'obbligo di adottare le misure di sicurezza è ribadito dall'articolo 31 del nuovo codice, che disciplina quelle che sono comunemente definite le ***misure idonee di sicurezza***, in merito alle quali sottolinea che "la norma impone al titolare e al Responsabile, se designato, l'obbligo di custodire e controllare i dati personali oggetto di trattamento mediante l'adozione di idonee e preventive misure di sicurezza, individuabili alla luce delle conoscenza acquisite in base al progresso tecnico in relazione alla natura dei dati ed alle specifiche caratteristiche del trattamento, in grado di ridurre al minimo i rischi".

Si tratta in sostanza dell'obbligo di operare in concreto al fine di ridurre al minimo i rischi mediante l'utilizzazione di sistemi di sicurezza *costantemente adeguati nel tempo*".

Le misure idonee sono quindi "*...non individuate*, ma *individuabili* sulla base delle soluzioni tecniche concretamente disponibili, e la loro mancata predisposizione comporta la Responsabilità per i danni eventualmente cagionati....".

In questo contesto, il Codice fa la distinzione tra:

- le cosiddette ***misure idonee*** (*Capo I del Titolo V della parte I*), che consistono in generale nell'insieme degli accorgimenti che il soggetto che tratta i dati deve adottare, in relazione alla sua specifica situazione, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Dalla mancata adozione, di tali misure, consegue l'obbligo di risarcimento dei danni eventualmente causati;
- le ***misure minime*** (Capo II del Titolo V della parte I), che il comma 3, lettera a) dell'articolo 4 definisce come il complesso delle misure tecniche, informatiche, organizzative, logistiche (leggasi logiche, NdR) e procedurali di sicurezza che configurano il livello minimo di protezione, richiesto in relazione ai rischi previsti nell'articolo 31. La loro adozione è imposta dalla norma, che provvede a descriverle analiticamente, con la conseguenza che sono previste sanzioni di natura penale, in caso di mancata adozione.

In merito alle misure che si devono in concreto adottare, il testo legislativo si limita genericamente a prevedere che si debbano applicare gli strumenti e le conoscenze resi disponibili dal progresso tecnico: non è quindi sufficiente impiantare una serie di misure di sicurezza una volta per tutte, ma ci si deve preoccupare di aggiornarle costantemente.

Tale principio, che è generale e vale quindi per tutte le misure di sicurezza, incluse quelle *fisiche* in senso stretto, assume particolare rilievo per le misure logiche legate al mondo informatico, in relazione al continuo progresso cui esso è soggetto, anche per quanto riguarda la creazione e circolazione di programmi concepiti per violare la altrui sicurezza.

2.3 Gli interventi formativi-informativi degli Incaricati

Gli interventi formativi degli Incaricati del trattamento devono essere programmati in modo tale, che essi abbiano luogo *almeno* al verificarsi di una delle seguenti circostanze:

- già al momento dell'ingresso in servizio;
- in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali;
- in occasione della introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti rispetto al trattamento di dati personali.

Gli interventi formativi, che possono avvenire all'interno e/o presso soggetti esterni specializzati, devono essere finalizzati a rendere gli Incaricati edotti dei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali, più rilevanti in rapporto alle relative attività, e conseguenti Responsabilità che ne derivano;
- rischi che incombono sui dati;
- misure disponibili per prevenire eventi dannosi;
- modalità per aggiornarsi sulle misure minime di sicurezza, adottate dal titolare.

Gli interventi formativi sono una importante componente della più vasta cultura della sicurezza, nel trattamento del patrimonio informativo dell'organizzazione, con particolare riferimento ai dati personali.

2.3.1 Sensibilizzazione e corresponsabilizzazione

La *sensibilizzazione* alle tematiche della sicurezza, ed a costanti comportamenti coerenti con le disposizioni date in merito, deve interessare tutte le risorse umane dell'organizzazione, ad ogni livello di Responsabilità ed attività: ciò al fine di diffondere una cultura generalizzata della sicurezza, che consenta tra l'altro di favorire la miglior efficacia ed efficienza delle misure prese, oltre che di sopperire ad eventuali mancanze delle stesse.

I Responsabili devono tenere presente che le attività relative alla sicurezza non rappresentano un appesantimento del lavoro quotidiano, ma una volta che entrano nel ciclo standard delle operazioni da compiere, contribuiscono a garantire il personale dal rischio di perdere, o comunque compromettere, parte del lavoro fatto.

A titolo di esempio, presentazioni, opuscoli, seminari, riunioni dei dirigenti con i propri collaboratori possono rappresentare opportunità per raggiungere quest'obiettivo.

Per la corresponsabilizzazione, si deve prevedere di:

- coinvolgere i dirigenti e le rappresentanze degli addetti, in tutte le fasi di definizione del piano per la sicurezza
- effettuare interventi di richiamo, e se necessario adottare gli adeguati provvedimenti disciplinari, in caso di inadempienze e/o superficialità in tema di sicurezza.

Analoghi processi devono essere previsti con eventuali partner e per i collaboratori esterni, privati e pubblici, persone fisiche e giuridiche, che interagiscono in modo significativo con l'organizzazione.

2.3.2 Formazione

L'introduzione di un sistema di sicurezza, come di qualunque altro elemento che modifichi le modalità lavorative all'interno di una qualsiasi realtà, ha sicuramente un forte impatto sull'organizzazione.

La formazione interviene in due momenti ben precisi del processo di introduzione di un sistema di sicurezza:

- sensibilizzazione sulle problematiche della sicurezza e sulla loro importanza;
- conoscenza delle misure di sicurezza da adottare, e da gestire ai diversi livelli di Responsabilità.

La formazione, se ben orientata, progettata e realizzata, può essere lo strumento più efficace per realizzare la diffusione delle politiche, degli obiettivi e dei piani dell'organizzazione in tema di sicurezza e per minimizzare quella componente, sempre presente, che consiste nella resistenza al cambiamento.

2.4 La protezione di aree e locali

E' l'insieme delle misura di sicurezza che hanno il compito di prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento del lavoro con gli strumenti automatizzati: la protezione delle aree e dei locali, in cui sono situati gli elaboratori, deve essere quindi attivata sia contro eventi dannosi imprevedibili (inondazioni, corti circuiti, ecc.), che contro tentativi di intrusione.

Le contromisure si riferiscono alle protezioni perimetrali dei siti, ai controlli fisici all'accesso, alla sicurezza delle aree dove sono collocati computer (con particolare riferimento a servers) rispetto a danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti.

Tale obiettivo viene raggiunto attraverso misure di controllo crescenti, correlate ai rischi e al valore dei beni e delle informazioni presenti nell'ambiente. Ne fanno parte le seguenti componenti:

- la classificazione delle aree aziendali (es: aree riservate, aree interne, aree pubbliche);
- l'accesso controllato alle aree considerate critiche;
- la sicurezza fisica (impianti) e la sorveglianza di queste aree;
- la tempestiva rilevazione di eventuali incidenti di sicurezza.

2.5 La custodia e l'archiviazione di atti, documenti e supporti

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti removibili di memorizzazione dei dati (ad esempio Tape, CD, dischetti, ecc.), i Responsabili dovranno provvedere ad istruire gli Incaricati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti.

Agli Incaricati verranno date disposizioni di accedere ai soli dati personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati: in caso di dubbi, essi si dovranno rivolgere ad un superiore, o ad un Responsabile del trattamento, o direttamente al titolare.

Agli Incaricati è prescritto di prelevare dagli archivi i soli atti e documenti che vengono loro affidati per lo svolgimento delle mansioni lavorative, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio, al termine di tale ciclo.

Gli Incaricati devono custodire in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative.

Cautele particolari devono essere previste per gli atti, documenti e supporti contenenti dati sensibili e giudiziari: agli Incaricati viene in questi casi prescritto di provvedere al controllo ed alla custodia in modo tale, che ai dati non possano accedere persone prive di autorizzazione. A tale fine, gli Incaricati sono stati dotati di:

- cassetti con serratura;
- armadi e schedari chiudibili a chiave

nei quali devono riporre i documenti, contenenti dati sensibili o giudiziari, prima di assentarsi dal posto di lavoro, anche temporaneamente. In tali dispositivi i documenti possono essere riposti anche al termine della giornata di lavoro, qualora l'Incaricato debba continuare ad utilizzarli, nei giorni successivi.

Al termine del trattamento, l'Incaricato dovrà restituire all'archivio gli atti, i documenti ed i supporti, non più necessari per lo svolgimento delle proprie mansioni lavorative.

Gli archivi contenenti dati sensibili o giudiziari devono essere controllati, mediante l'adozione dei seguenti accorgimenti:

- le persone vengono autorizzate preventivamente ad accedere agli archivi, previa richiesta della chiave all'Incaricato che ha il compito di custodirla;

- si procede inoltre ad identificare e registrare le persone che accedono agli archivi, contenenti dati sensibili o giudiziari, dopo l'orario di chiusura degli uffici, mediante (ad esempio) l'adozione del seguente accorgimento:
- la chiave dell'archivio è affidata, dopo l'orario di chiusura, al titolare o ai Responsabili del trattamento, o in alternativa ad uno o più soggetti Incaricati per iscritto, i quali provvedono ad annotare in un apposito registro i nominativi di coloro che hanno richiesto di accedere all'archivio;
- I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

Per qualsiasi tipo di documento o semilavorato cartaceo che contenga dati sensibili e giudiziari, quando non più utilizzati, è prescritto che vengano definitivamente distrutti in modo che le informazioni in essi contenuti non siano intelligibili.

2.6 Le misure logiche di sicurezza nell'utilizzo degli strumenti elettronici

Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), si adottano le seguenti misure:

- utilizzo di un **sistema di autenticazione informatica**, che ha il fine di accertare l'identità delle persone atte a svolgere un determinato trattamento, in modo che possano accedere ai dati personali le sole persone autorizzate
- utilizzo di un **sistema di autorizzazione**, che ha il fine di circoscrivere le tipologie di dati ai quali gli Incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative
- gestione di un **sistema di protezione**, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus)
- prescrizione delle **opportune cautele per la custodia e l'utilizzo** dei supporti rimovibili (floppy disk, dischi ZIP, CD....), nei quali siano contenuti dati personali.

2.6.1 Le credenziali di autenticazione informatica

Il sistema di autenticazione informatica viene adottato per disciplinare gli accessi a tutti gli strumenti elettronici, presenti nell'organizzazione del Titolare, fatta unicamente salva l'eventuale eccezione per quelli che:

- non contengono dati personali;
- contengono solo dati personali destinati alla diffusione, che sono quindi per definizione conoscibili da chiunque.

Per tutti gli altri casi, è impostata e gestita una procedura di autenticazione, che permette di verificare l'identità della persona, e quindi di accertare che la stessa è in possesso delle credenziali di autenticazione per accedere ad un determinato strumento elettronico col quale trattare i dati personali.

Per realizzare le credenziali di autenticazione si utilizza il seguente metodo:

- si associa un codice per l'identificazione dell'Incaricato (username), attribuito da chi amministra il sistema, ad una parola chiave riservata (password), conosciuta esclusivamente dall'Incaricato, che provvederà, in piena autonomia, ad elaborarla, mantenerla riservata e modificarla periodicamente.

Per l'attribuzione e la gestione delle credenziali per l'autenticazione si utilizza il seguente criterio:

- esse vengono assegnate ad ogni Incaricato individualmente, per cui non è ammesso che due o più Incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale.

Nei casi in cui una componente della credenziale di autenticazione è costituita dal codice per l'identificazione (username), attribuito all'Incaricato da chi amministra il sistema, tale codice deve essere univoco: esso non può essere assegnato ad altri Incaricati, neppure in tempi diversi.

E' invece ammesso, qualora sia necessario o comunque opportuno, che ad una persona venga assegnata più di una credenziale di autenticazione.

2.6.2 La disattivazione delle credenziali di autenticazione

Al verificarsi dei seguenti casi, è prevista la disattivazione delle credenziali di autenticazione:

- immediatamente, nel caso in cui l'Incaricato perda la qualità, che gli consentiva di accedere allo strumento;
- in ogni caso, entro sei mesi di mancato utilizzo, con l'unica eccezione delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo è quindi sporadico.

2.6.3 Le istruzioni agli Incaricati

Agli Incaricati vengono impartite precise istruzioni in merito ai seguenti punti:

- obbligo di custodire i dispositivi, attribuiti agli Incaricati a titolo di possesso ed uso esclusivo, con i quali si può accedere agli strumenti informatici (ad esempio, il tesserino magnetico o la smart card): la custodia deve avvenire in modo diligente, sia nell'ipotesi in cui tali dispositivi siano riposti negli uffici (viene prescritto l'obbligo di utilizzare cassetti con serratura), che in quella in cui l'Incaricato provveda a portare il dispositivo con sé (viene prescritto l'obbligo di custodirlo come se fosse una carta di credito); in ipotesi di smarrimento, l'Incaricato deve provvedere immediatamente a segnalare la circostanza all'amministratore di sistema, o alle altre persone che sono state a tale fine indicate, al momento dell'attribuzione del dispositivo;
- obbligo di non lasciare incustodito e accessibile lo strumento elettronico, durante una sessione di trattamento, neppure in ipotesi di breve assenza;
- obbligo di elaborare in modo appropriato la password e di conservare la segretezza sulla stessa; agli Incaricati è imposto l'obbligo di provvedere a modificare la password, con la seguente tempistica:
  - immediatamente, non appena viene consegnata loro da chi amministra il sistema;
  - successivamente, almeno ogni sei mesi. Tale termine scende a tre mesi, se la password dà accesso ad aree in cui sono contenuti dati sensibili o giudiziari.
- prescrizione di comporre password di **almeno otto caratteri,** oppure, nel caso in cui lo strumento elettronico non permetta una tale lunghezza, da un numero di caratteri pari al massimo consentito dallo strumento stesso;
- prescrizione di **non utilizzare** per le password, nomi semplici o riferimenti agevolmente riconducibili all'interessato (nomi, cognomi, soprannomi, date di nascita proprie, di figli, ecc.);
- obbligo di segretezza della password, ossia di non comunicarla a nessuno (non solo a soggetti esterni, ma neppure a persone appartenenti all'organizzazione, siano esse colleghi, Responsabili del trattamento, amministratore del sistema o titolare).

2.6.4 La gestione password in deroga

Nei casi di prolungata assenza o impedimento dell'Incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe rendersi necessario

disporre della password dell'Incaricato, per accedere agli strumenti ed ai dati. A tale fine, agli Incaricati viene richiesto di:

- scrivere la parola chiave su un foglio di carta, da inserire in una busta che deve essere chiusa e sigillata;
- consegnare la busta alla persona preventivamente preposta allo scopo mediante incarico formale.

Solo al verificarsi delle condizioni, sopra esposte, che rendono necessario accedere allo strumento elettronico, utilizzando la copia della parola chiave, il titolare o un Responsabile potranno richiedere la busta che la contiene, a chi la custodisce. Dell'accesso effettuato si dovrà provvedere ad informare, tempestivamente, l'Incaricato cui appartiene la parola chiave.

2.6.5 I profili di autorizzazione

Per discriminare le tipologie di dati ai quali ciascun Incaricato può accedere ed i trattamenti che può effettuare, si è impostato un sistema di autorizzazione, che circoscrive la sfera d'azione di ciascuno ai dati e ai trattamenti strettamente necessari per lo svolgimento delle proprie mansioni lavorative.

L'unica eccezione si ha nei casi in cui il trattamento riguardi solo dati personali destinati alla diffusione: in questo caso non è necessario predisporre alcun sistema di autorizzazione, poiché i dati trattati sono, per definizione, conoscibili da chiunque.

Al di fuori di questi casi, le autorizzazioni all'accesso vengono rilasciate e revocate dal titolare e, se designato, dal Responsabile della sicurezza, ovvero da soggetti da questi appositamente incaricati.

Il profilo di autorizzazione non viene studiato per ogni singolo Incaricato, ma è impostato per classi omogenee di Incaricati (ad esempio, attribuendo un determinato profilo di autorizzazione a tutti gli impiegati della contabilità, ed attribuendone un altro a coloro che lavorano nell'ufficio personale).

L'obiettivo di fondo, in ogni caso, è di limitare preventivamente l'accesso, di ciascun Incaricato o di ciascuna classe omogenea di Incaricati, ai soli dati necessari per effettuare le operazioni di trattamento, che sono indispensabili per svolgere le mansioni lavorative.

2.6.6 La verifica periodica di sussistenza

Periodicamente, e comunque almeno annualmente, viene verificata la sussistenza delle condizioni per la conservazione delle credenziali di autenticazione e dei profili di autorizzazione: ciò per quanto riguarda l'ambito di trattamento consentito sia ai singoli Incaricati, che agli addetti alla manutenzione e gestione degli strumenti elettronici.

2.6.7 La protezione anti-intrusione e anti-virus

Per quanto riguarda la protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi antivirus che contengono codici maliziosi (virus, trojan, backdoor, etc.), devono essere adottati idonei strumenti elettronici e programmi, che il Dlgs 196/2003 imporrebbe di aggiornare con cadenza almeno semestrale, ma che, in relazione al continuo evolversi dei virus, si è ritenuto opportuno di sottoporre ad aggiornamento, di regola:

- Indicativamente ogni settimana nel caso di strumenti elettronici in rete;

Indicativamente ogni sei mesi nel caso di strumenti elettronici che non sono in rete.

Tutti gli Incaricati devono essere stati istruiti, in merito all'utilizzo dei programmi antivirus e, più in generale, sulle norme di comportamento da tenere per minimizzare il rischio di essere contagiati: a tale fine, dovrà essere loro distribuito un codice dei comportamenti da tenere e di quelli da evitare.

Occorre provvedere anche alla protezione degli elaboratori in rete dall'accesso abusivo, di cui all'articolo 615-ter del codice penale, ai sensi del quale compie tale reato chi si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

La protezione da tali accessi avviene mediante l'impiego di idonei strumenti elettronici, comunemente conosciuti come firewall e anti-spyware.

A tale riguardo Azienda Ospedaliero Universitario è dotata di più firewall che limitano l'accesso alla rete aziendale dall'esterno a servizi e utenti non autorizzati.

Inoltre sono impartite istruzioni agli amministratori dei vari sistemi (interni o esterni) di tenersi aggiornati periodicamente sui programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti (fix, patch, service pack, ecc.).

L'aggiornamento è effettuato almeno annualmente ed in caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

2.6.8 La gestione dei supporti fisici rimovibili

Per quanto concerne i supporti fisici rimovibili (es. floppy disk, dischi ZIP, CD....), contenenti dati personali, la norma impone che siano impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

I Responsabili devono prescrivere agli Incaricati del trattamento quanto segue:

- i supporti devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono essere conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati o distrutti, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi;
- una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.

3 L'affidamento di dati personali all'esterno

Nei casi in cui i trattamenti di dati personali vengano affidati, in conformità a quanto previsto dal Dlgs 196/2003, all'esterno della struttura del Titolare, si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime, previste dagli articoli da 33 a 35 Dlgs 196/2003 e dal disciplinare tecnico, allegato sub b) al codice.

Per la generalità dei casi, in cui il trattamento di dati personali, di qualsiasi natura, venga affidato all'esterno della struttura del titolare, sono impartite istruzioni per iscritto al terzo destinatario, di rispettare quanto prescritto per il trattamento dei dati personali:

- dal D. lgs. 196/2003, se il terzo destinatario è italiano;
- dalla direttiva 95/46/CE , se il terzo destinatario non è italiano.

3.1 Dichiarazione di assunzione di Responsabilità

In ogni caso, il soggetto cui le attività sono affidate dichiara:

- di essere consapevole che i dati che tratterà, nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali, sono soggetti all'applicazione della normativa per la protezione dei dati personali;
- di ottemperare agli obblighi previsti dalla normativa per la protezione dei dati personali;
- di attenersi alle istruzioni specifiche, eventualmente ricevute per il trattamento dei dati personali, conformando ad esse anche le procedure eventualmente già in essere;
- di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate, e di avvertire immediatamente il proprio committente in caso di situazioni anomale o di emergenze;
- di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

Nell'ipotesi in cui il trattamento, di dati sensibili o giudiziari, avvenga con strumenti elettronici, si esige inoltre che il destinatario italiano:

- rilasci la dichiarazione di avere redatto il documento programmatico sulla sicurezza, nel quale abbia attestato di avere adottato le misure minime previste dal disciplinare tecnico.

Nei casi in cui ciò si renda opportuno, per ragioni operative legate anche alla tutela dei dati personali, il destinatario esterno viene nominato dal Titolare come Responsabile del trattamento dei dati, mediante apposita lettera scritta.

3.2 Trasferimento di dati a soggetti in paesi extra-UE

Qualora il trasferimento dovesse avvenire verso soggetti residenti in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, si stipulano con il destinatario clausole contrattuali conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE: eccezione può essere fatta nei casi, previsti dall'articolo 43 Dlgs 196/2003, in cui il trasferimento può avvenire senza che vengano stipulate tali clausole.

Nei casi in cui il trattamento affidato all'esterno abbia per oggetto dati **sensibili o giudiziari**, si procede alla stipula di clausole contrattuali, con il destinatario, che disciplinano gli aspetti legati alla gestione dei dati personali: se il destinatario è residente in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, tali clausole sono conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE.

4 Il controllo generale sullo stato della sicurezza

Al Responsabile per la Sicurezza Informatica è affidato il compito di aggiornare le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnologico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.

Al fine di verificare l'efficacia delle misure di sicurezza adottate, il Responsabile o i suoi Incaricati provvederanno periodicamente, anche con controlli a campione, ad effettuare una o più delle seguenti attività, rilevando le eventuali non conformità riscontrate:

- verificare l'accesso fisico ai locali dove sono situati i sistemi informatici e le stazioni di lavoro utilizzati per i trattamenti;
- verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici, mediante l'analisi dei log file, nei quali i software di sicurezza installati, i sistemi operativi e le applicazioni scrivono le operazioni svolte dagli Incaricati per il loro tramite. Attraverso questa analisi è possibile individuare i tentativi, riusciti o meno, di accesso al sistema e l'esecuzione di operazioni non corrette, o sospette;
- verificare l'integrità dei dati e delle loro copie di backup;
- verificare la sicurezza delle trasmissioni in rete;
- verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti;
- verificare il livello di formazione degli Incaricati.

Almeno ogni sei mesi, si procederà ad una sistematica verifica del corretto utilizzo delle parole chiave e dei profili di autorizzazione che consentono l'accesso agli strumenti elettronici da parte degli Incaricati, anche al fine di disabilitare quelli che non sono stati mai utilizzati in sei mesi.

Dell'attività di verifica svolta sarà redatto un verbale, che sarà messo a disposizione del Titolare.

5 Appendice

5.1 Indice del TU

5.2 Estratto del D. lgs. 196/03 – Parte II – Titolo V

Per comodità viene riportato un estratto del Codice che riguarda specificatamente il trattamento di dati personali in ambito sanitario:

TITOLO V - TRATTAMENTO DI DATI PERSONALI IN AMBITO SANITARIO

5.3 CAPO I - PRINCIPI GENERALI

Art. 75 (Ambito applicativo)

1. *Il presente titolo disciplina il trattamento dei dati personali in ambito sanitario.*

Art. 76 (Esercenti professioni sanitarie e organismi sanitari pubblici)

1. *Gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, anche nell'ambito di un'attività di rilevante interesse pubblico ai sensi dell'articolo 85, trattano i dati personali idonei a rivelare lo stato di salute:*
   a) *con il consenso dell'interessato e anche senza l'autorizzazione del Garante, se il trattamento riguarda dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato;*
   b) *anche senza il consenso dell'interessato e previa autorizzazione del Garante, se la finalità di cui alla lettera a) riguarda un terzo o la collettività.*
2. *Nei casi di cui al comma 1 il consenso può essere prestato con le modalità semplificate di cui al capo II.*
3. *Nei casi di cui al comma 1 l'autorizzazione del Garante è rilasciata, salvi i casi di particolare urgenza, sentito il Consiglio superiore di sanità.*

5.4 CAPO II - MODALITA' SEMPLIFICATE PER INFORMATIVA E CONSENSO

Art. 77 (Casi di semplificazione)

1. *Il presente capo individua modalità semplificate utilizzabili dai soggetti di cui al comma 2:*
   a) *per informare l'interessato relativamente ai dati personali raccolti presso il medesimo interessato o presso terzi, ai sensi dell'articolo 13, commi 1 e 4;*
   b) *per manifestare il consenso al trattamento dei dati personali nei casi in cui ciò è richiesto ai sensi dell'articolo 76;*
   c) *per il trattamento dei dati personali.*
2. *Le modalità semplificate di cui al comma 1 sono applicabili:*
   a) *dagli organismi sanitari pubblici;*
   b) *dagli altri organismi privati e dagli esercenti le professioni sanitarie;*
   c) *dagli altri soggetti pubblici indicati nell'articolo 80.*

Art. 78 (Informativa del medico di medicina generale o del pediatra)

1. *Il medico di medicina generale o il pediatra di libera scelta informano l'interessato relativamente al trattamento dei dati personali, in forma chiara e tale da rendere agevolmente comprensibili gli elementi indicati nell'articolo 13, comma 1.*
2. *L'informativa può essere fornita per il complessivo trattamento dei dati personali necessario per attività di prevenzione, diagnosi, cura e riabilitazione, svolte dal medico o dal pediatra a tutela della salute o dell'incolumità fisica dell'interessato, su richiesta dello stesso o di cui questi è informato in quanto effettuate nel suo interesse.*

3. *L'informativa può riguardare, altresì, dati personali eventualmente raccolti presso terzi, ed è fornita preferibilmente per iscritto, anche attraverso carte tascabili con eventuali allegati pieghevoli, includendo almeno gli elementi indicati dal Garante ai sensi dell'articolo 13, comma 3, eventualmente integrati anche oralmente in relazione a particolari caratteristiche del trattamento.*

4. *L'informativa, se non è diversamente specificato dal medico o dal pediatra, riguarda anche il trattamento di dati correlato a quello effettuato dal medico di medicina generale o dal pediatra di libera scelta, effettuato da un professionista o da altro soggetto, parimenti individuabile in base alla prestazione richiesta, che:*

   a) sostituisce temporaneamente il medico o il pediatra;

   b) fornisce una prestazione specialistica su richiesta del medico e del pediatra;

   c) può trattare lecitamente i dati nell'ambito di un'attività professionale prestata in forma associata;

   d) fornisce farmaci prescritti;

   e) comunica dati personali al medico o pediatra in conformità alla disciplina applicabile.

5. *L'informativa resa ai sensi del presente articolo evidenzia analiticamente eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in particolare in caso di trattamenti effettuati:*

   a) per scopi scientifici, anche di ricerca scientifica e di sperimentazione clinica controllata di medicinali, in conformità alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente;

   b) nell'ambito della teleassistenza o telemedicina;

   c) per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica.

Art. 79 (Informativa da parte di organismi sanitari)

1. *Gli organismi sanitari pubblici e privati possono avvalersi delle modalità semplificate relative all'informativa e al consenso di cui agli articoli 78 e 81 in riferimento ad una pluralità di prestazioni erogate anche da distinti reparti ed unità dello stesso organismo o di più strutture ospedaliere o territoriali specificamente identificati.*

2. *Nei casi di cui al comma 1 l'organismo o le strutture annotano l'avvenuta informativa e il consenso con modalità uniformi e tali da permettere una verifica al riguardo da parte di altri reparti ed unità che, anche in tempi diversi, trattano dati relativi al medesimo interessato.*

3. *Le modalità semplificate di cui agli articoli 78 e 81 possono essere utilizzate in modo omogeneo e coordinato in riferimento all'insieme dei trattamenti di dati personali effettuati nel complesso delle strutture facenti capo alle aziende sanitarie.*

4. *Sulla base di adeguate misure organizzative in applicazione del comma 3, le modalità semplificate possono essere utilizzate per più trattamenti di dati effettuati nei casi di cui al presente articolo e dai soggetti di cui all'articolo 80.*

Art. 80 (Informativa da parte di altri soggetti pubblici)

1. *Oltre a quanto previsto dall'articolo 79, possono avvalersi della facoltà di fornire un' unica informativa per una pluralità di trattamenti di dati effettuati, a fini amministrativi e in tempi diversi, rispetto a dati raccolti presso l'interessato e presso terzi, i competenti servizi o strutture di soggetti pubblici operanti in ambito sanitario o della prevenzione e sicurezza del lavoro.*

2. *L'informativa di cui al comma 1 è integrata con appositi e idonei cartelli ed avvisi agevolmente visibili al pubblico, affissi e diffusi anche nell'ambito di pubblicazioni istituzionali e mediante reti di comunicazione elettronica, in particolare per quanto riguarda attività amministrative di rilevante interesse pubblico che non richiedono il consenso degli interessati.*

Art. 81 (Prestazione del consenso)

1. *Il consenso al trattamento dei dati idonei a rivelare lo stato di salute, nei casi in cui è necessario ai sensi del presente codice o di altra disposizione di legge, può essere manifestato con un'unica dichiarazione, anche oralmente. In tal caso il consenso è documentato, anziché con atto scritto dell'interessato, con*

annotazione dell'esercente la professione sanitaria o dell'organismo sanitario pubblico, riferita al trattamento di dati effettuato da uno o più soggetti e all'informativa all'interessato, nei modi indicati negli articoli 78, 79 e 80.

2. *Quando il medico o il pediatra fornisce l'informativa per conto di più professionisti ai sensi dell'articolo 78, comma 4, oltre quanto previsto dal comma 1, il consenso è reso conoscibile ai medesimi professionisti con adeguate modalità, anche attraverso menzione, annotazione o apposizione di un bollino o tagliando su una carta elettronica o sulla tessera sanitaria, contenente un richiamo al medesimo articolo 78, comma 4, e alle eventuali diverse specificazioni apposte all'informativa ai sensi del medesimo comma.*

Art. 82 (Emergenze e tutela della salute e dell'incolumità fisica)

1. *L'informativa e il consenso al trattamento dei dati personali possono intervenire senza ritardo, successivamente alla prestazione, nel caso di emergenza sanitaria o di igiene pubblica per la quale la competente autorità ha adottato un'ordinanza contingibile ed urgente ai sensi dell'articolo 117 del decreto legislativo 31 marzo 1998, n. 112.*
2. *L'informativa e il consenso al trattamento dei dati personali possono altresì intervenire senza ritardo, successivamente alla prestazione, in caso di:*

a) impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile acquisire il consenso da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato;

b) rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'interessato.

3. *L'informativa e il consenso al trattamento dei dati personali possono intervenire senza ritardo, successivamente alla prestazione, anche in caso di prestazione medica che può essere pregiudicata dall'acquisizione preventiva del consenso, in termini di tempestività o efficacia.*
4. *Dopo il raggiungimento della maggiore età l'informativa è fornita all'interessato anche ai fini della acquisizione di una nuova manifestazione del consenso quando questo è necessario.*

Art. 83 (Altre misure per il rispetto dei diritti degli interessati)

1. *I soggetti di cui agli articoli 78, 79 e 80 adottano idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalle leggi e dai regolamenti in materia di modalità di trattamento dei dati sensibili e di misure minime di sicurezza.*
2. *Le misure di cui al comma 1 comprendono, in particolare:*
   a) *soluzioni volte a rispettare, in relazione a prestazioni sanitarie o ad adempimenti amministrativi preceduti da un periodo di attesa all'interno di strutture, un ordine di precedenza e di chiamata degli interessati prescindendo dalla loro individuazione nominativa;*
   b) *l'istituzione di appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere;*
   c) *soluzioni tali da prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute;*
   d) *cautele volte ad evitare che le prestazioni sanitarie, ivi compresa l'eventuale documentazione di anamnesi, avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti;*
   e) *il rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dei dati;*
   f) *la previsione di opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati, di una prestazione di pronto soccorso;*
   g) *la formale previsione, in conformità agli ordinamenti interni delle strutture ospedaliere e territoriali, di adeguate modalità per informare i terzi legittimati in occasione di visite sulla dislocazione degli*

interessati nell'ambito dei reparti, informandone previamente gli interessati e rispettando eventuali loro contrarie manifestazioni legittime di volontà;

h) la messa in atto di procedure, anche di formazione del personale, dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute;

i) la sottoposizione degli incaricati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale.

Art. 84 (Comunicazione di dati all'interessato)

1. *I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato o ai soggetti di cui all'articolo 82, comma 2, lettera a), da parte di esercenti le professioni sanitarie ed organismi sanitari, solo per il tramite di un medico designato dall'interessato o dal titolare. Il presente comma non si applica in riferimento ai dati personali forniti in precedenza dal medesimo interessato.*
2. *Il titolare o il responsabile possono autorizzare per iscritto esercenti le professioni sanitarie diversi dai medici, che nell'esercizio dei propri compiti intrattengono rapporti diretti con i pazienti e sono incaricati di trattare dati personali idonei a rivelare lo stato di salute, a rendere noti i medesimi dati all'interessato o ai soggetti di cui all'articolo 82, comma 2, lettera a). L'atto di incarico individua appropriate modalità e cautele rapportate al contesto nel quale è effettuato il trattamento di dati.*

5.5 CAPO III - FINALITA' DI RILEVANTE INTERESSE PUBBLICO

Art. 85 (Compiti del Servizio sanitario nazionale)

1. *Fuori dei casi di cui al comma 2, si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità che rientrano nei compiti del Servizio sanitario nazionale e degli altri organismi sanitari pubblici relative alle seguenti attività:*
   a) attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione dei soggetti assistiti dal Servizio sanitario nazionale, ivi compresa l'assistenza degli stranieri in Italia e dei cittadini italiani all'estero, nonché di assistenza sanitaria erogata al personale navigante ed aeroportuale;
   b) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria;
   c) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;
   d) attività certificatorie;
   e) l'applicazione della normativa in materia di igiene e sicurezza nei luoghi di lavoro e di sicurezza e salute della popolazione;
   f) le attività amministrative correlate ai trapianti d'organo e di tessuti, nonché alle trasfusioni di sangue umano, anche in applicazione della legge 4 maggio 1990, n. 107;
   g) instaurazione, gestione, pianificazione e controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati del Servizio sanitario nazionale.
2. *Il comma 1 non si applica ai trattamenti di dati idonei a rivelare lo stato di salute effettuati da esercenti le professioni sanitarie o da organismi sanitari pubblici per finalità di tutela della salute o dell'incolumità fisica dell'interessato, di un terzo o della collettività, per i quali si osservano le disposizioni relative al consenso dell'interessato o all'autorizzazione del Garante ai sensi dell'articolo 76.*
3. *All'identificazione dei tipi di dati idonei a rivelare lo stato di salute e di operazioni su essi eseguibili è assicurata ampia pubblicità, anche tramite affissione di una copia o di una guida illustrativa presso ciascuna azienda sanitaria e presso gli studi dei medici di medicina generale e dei pediatri di libera scelta.*
4. *Il trattamento di dati identificativi dell'interessato è lecito da parte dei soli soggetti che perseguono direttamente le finalità di cui al comma 1. L'utilizzazione delle diverse tipologie di dati è consentita ai soli incaricati, preposti, caso per caso, alle specifiche fasi delle attività di cui al medesimo comma, secondo il principio dell'indispensabilità dei dati di volta in volta trattati.*

Art. 86 (Altre finalità di rilevante interesse pubblico)

1. *Fuori dei casi di cui agli articoli 76 e 85, si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità, perseguite mediante trattamento di dati sensibili e giudiziari, relative alle attività amministrative correlate all'applicazione della disciplina in materia di:*
   a) tutela sociale della maternità e di interruzione volontaria della gravidanza, con particolare riferimento a quelle svolte per la gestione di consultori familiari e istituzioni analoghe, per l'informazione, la cura e la degenza delle madri, nonché per gli interventi di interruzione della gravidanza;
   b) stupefacenti e sostanze psicotrope, con particolare riferimento a quelle svolte al fine di assicurare, anche avvalendosi di enti ed associazioni senza fine di lucro, i servizi pubblici necessari per l'assistenza socio-sanitaria ai tossicodipendenti, gli interventi anche di tipo preventivo previsti dalle leggi e l'applicazione delle misure amministrative previste;
   c) assistenza, integrazione sociale e diritti delle persone handicappate effettuati, in particolare, al fine di:
      1) accertare l'handicap ed assicurare la funzionalità dei servizi terapeutici e riabilitativi, di aiuto personale e familiare, nonché interventi economici integrativi ed altre agevolazioni;
      2) curare l'integrazione sociale, l'educazione, l'istruzione e l'informazione alla famiglia del portatore di handicap, nonché il collocamento obbligatorio nei casi previsti dalla legge;
      3) realizzare comunità-alloggio e centri socio riabilitativi;
      4) curare la tenuta degli albi degli enti e delle associazioni ed organizzazioni di volontariato impegnati nel settore.
2. *Ai trattamenti di cui al presente articolo si applicano le disposizioni di cui all'articolo 85, comma 4.*

5.6 CAPO IV - PRESCRIZIONI MEDICHE

Art. 87 (Medicinali a carico del Servizio sanitario nazionale)

1. *Le ricette relative a prescrizioni di medicinali a carico, anche parziale, del Servizio sanitario nazionale sono redatte secondo il modello di cui al comma 2, conformato in modo da permettere di risalire all'identità dell'interessato solo in caso di necessità connesse al controllo della correttezza della prescrizione, ovvero a fini di verifiche amministrative o per scopi epidemiologici e di ricerca, nel rispetto delle norme deontologiche applicabili.*
2. *Il modello cartaceo per le ricette di medicinali relative a prescrizioni di medicinali a carico, anche parziale, del Servizio sanitario nazionale, di cui agli allegati 1, 3, 5 e 6 del decreto del Ministro della sanità 11 luglio 1988, n. 350, e al capitolo 2, paragrafo 2.2.2. del relativo disciplinare tecnico, è integrato da un tagliando predisposto su carta o con tecnica di tipo copiativo e unito ai bordi delle zone indicate nel comma 3.*
3. *Il tagliando di cui al comma 2 è apposto sulle zone del modello predisposte per l'indicazione delle generalità e dell'indirizzo dell'assistito, in modo da consentirne la visione solo per effetto di una momentanea separazione del tagliando medesimo che risulti necessaria ai sensi dei commi 4 e 5.*
4. *Il tagliando può essere momentaneamente separato dal modello di ricetta, e successivamente riunito allo stesso, quando il farmacista lo ritiene indispensabile, mediante sottoscrizione apposta sul tagliando, per una effettiva necessità connessa al controllo della correttezza della prescrizione, anche per quanto riguarda la corretta fornitura del farmaco.*
5. *Il tagliando può essere momentaneamente separato nei modi di cui al comma 3 anche presso i competenti organi per fini di verifica amministrativa sulla correttezza della prescrizione, o da parte di soggetti legittimati a svolgere indagini epidemiologiche o di ricerca in conformità alla legge, quando è indispensabile per il perseguimento delle rispettive finalità.*
6. *Con decreto del Ministro della salute, sentito il Garante, può essere individuata una ulteriore soluzione tecnica diversa da quella indicata nel comma 1, basata sull'uso di una fascetta adesiva o su altra tecnica equipollente relativa anche a modelli non cartacei.*

Art. 88 (Medicinali non a carico del Servizio sanitario nazionale)

1. *Nelle prescrizioni cartacee di medicinali soggetti a prescrizione ripetibile non a carico, anche parziale, del Servizio sanitario nazionale, le generalità dell'interessato non sono indicate.*
2. *Nei casi di cui al comma 1 il medico può indicare le generalità dell'interessato solo se ritiene indispensabile permettere di risalire alla sua identità, per un'effettiva necessità derivante dalle particolari condizioni del medesimo interessato o da una speciale modalità di preparazione o di utilizzazione.*

Art. 89 (Casi particolari)

1. *Le disposizioni del presente capo non precludono l'applicazione di disposizioni normative che prevedono il rilascio di ricette che non identificano l'interessato o recanti particolari annotazioni, contenute anche nel decreto-legge 17 febbraio 1998, n. 23, convertito, con modificazioni, dalla legge 8 aprile 1998, n. 94.*
2. *Nei casi in cui deve essere accertata l'identità dell'interessato ai sensi del testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza, approvato con decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, e successive modificazioni, le ricette sono conservate separatamente da ogni altro documento che non ne richiede l'utilizzo.*

5.7 CAPO V - DATI GENETICI

Art. 90 (Trattamento dei dati genetici e donatori di midollo osseo)

1. *Il trattamento dei dati genetici da chiunque effettuato è consentito nei soli casi previsti da apposita autorizzazione rilasciata dal Garante sentito il Ministro della salute, che acquisisce, a tal fine, il parere del Consiglio superiore di sanità.*
2. *L'autorizzazione di cui al comma 1 individua anche gli ulteriori elementi da includere nell'informativa ai sensi dell'articolo 13, con particolare riguardo alla specificazione delle finalità perseguite e dei risultati conseguibili anche in relazione alle notizie inattese che possono essere conosciute per effetto del trattamento dei dati e al diritto di opporsi al medesimo trattamento per motivi legittimi.*
3. *Il donatore di midollo osseo, ai sensi della legge 6 marzo 2001, n. 52, ha il diritto e il dovere di mantenere l'anonimato sia nei confronti del ricevente sia nei confronti di terzi.*

5.8 CAPO VI - DISPOSIZIONI VARIE

Art. 91 (Dati trattati mediante carte)

1. *Il trattamento in ogni forma di dati idonei a rivelare lo stato di salute o la vita sessuale eventualmente registrati su carte anche non elettroniche, compresa la carta nazionale dei servizi, o trattati mediante le medesime carte è consentito se necessario ai sensi dell'articolo 3, nell'osservanza di misure ed accorgimenti prescritti dal Garante nei modi di cui all'articolo 17.*

Art. 92 (Cartelle cliniche)

1. *Nei casi in cui organismi sanitari pubblici e privati redigono e conservano una cartella clinica in conformità alla disciplina applicabile, sono adottati opportuni accorgimenti per assicurare la comprensibilità dei dati e per distinguere i dati relativi al paziente da quelli eventualmente riguardanti altri interessati, ivi comprese informazioni relative a nascituri.*
2. *Eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:*
   a) di far valere o difendere un diritto in sede giudiziaria ai sensi dell'articolo 26, comma 4, lettera c), di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

b) di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Art. 93 (Certificato di assistenza al parto)

1. *Ai fini della dichiarazione di nascita il certificato di assistenza al parto è sempre sostituito da una semplice attestazione contenente i soli dati richiesti nei registri di nascita. Si osservano, altresì, le disposizioni dell'articolo 109.*
2. *Il certificato di assistenza al parto o la cartella clinica, ove comprensivi dei dati personali che rendono identificabile la madre che abbia dichiarato di non voler essere nominata avvalendosi della facoltà di cui all'articolo 30, comma 1, del decreto del Presidente della Repubblica 3 novembre 2000, n. 396, possono essere rilasciati in copia integrale a chi vi abbia interesse, in conformità alla legge, decorsi cento anni dalla formazione del documento.*
3. *Durante il periodo di cui al comma 2 la richiesta di accesso al certificato o alla cartella può essere accolta relativamente ai dati relativi alla madre che abbia dichiarato di non voler essere nominata, osservando le opportune cautele per evitare che quest'ultima sia identificabile.*

Art. 94 (Banche di dati, registri e schedari in ambito sanitario)

1. *Il trattamento di dati idonei a rivelare lo stato di salute contenuti in banche di dati, schedari, archivi o registri tenuti in ambito sanitario, è effettuato nel rispetto dell'articolo 3 anche presso banche di dati, schedari, archivi o registri già istituiti alla data di entrata in vigore del presente codice e in riferimento ad accessi di terzi previsti dalla disciplina vigente alla medesima data, in particolare presso:*
   a) il registro nazionale dei casi di mesotelioma asbesto-correlati istituito presso l'Istituto superiore per la prevenzione e la sicurezza del lavoro (Ispesl), di cui all'articolo 1 del decreto del Presidente del Consiglio dei ministri 10 dicembre 2002, n. 308;
   b) la banca di dati in materia di sorveglianza della malattia di Creutzfeldt-Jakob o delle varianti e sindromi ad essa correlate, di cui al decreto del Ministro della salute in data 21 dicembre 2001, pubblicato nella Gazzetta Ufficiale n. 8 del 10 gennaio 2002;
   c) il registro nazionale delle malattie rare di cui all'articolo 3 del decreto del Ministro della sanità in data 18 maggio 2001, n. 279;
   d) i registri dei donatori di midollo osseo istituiti in applicazione della legge 6 marzo 2001, n. 52;
   e) gli schedari dei donatori di sangue di cui all'articolo 15 del decreto del Ministro della sanità in data 26 gennaio 2001, pubblicato nella Gazzetta Ufficiale n. 78 del 3 aprile 2001.

Segnalazioni e Suggerimenti

Questo documento dovrà evolversi per essere un utile strumento di lavoro, riflettendo i mutamenti dell'organizzazione e delle infrastrutture dell'AOU, e recependo le esigenze dei Responsabili e di tutti coloro che lo utilizzeranno.

Le Vostre segnalazioni e i Vostri suggerimenti sono molto importanti perché ciò avvenga.

Per farlo, potete inviare questo modulo debitamente compilato al Responsabile per la Sicurezza Informatica, che terrà in debito conto le Vostre osservazioni per migliorare le successive edizioni di questo documento.

Potete fotocopiare e compilare il modulo sottostante e quindi spedirlo all'indirizzo specificato, oppure inviare una e-mail con le stesse informazioni a sicurezza@aousassari.it

Data _____

Da: _____

Unità _____

_____

_____

Tel _____

A: Responsabile Sicurezza Informatica
Azienda Ospedaliero Universitaria
Direzione Generale
Via M. Coppino, 26
07100 - Sassari

e-mail _____

COMMENTI E SUGGERIMENTI:

- I contenuti del documento sono sufficientemente esaurienti in relazione alla finalità?

  Sì ☐ No ☐

- Quali punti o argomenti ritenete debbano essere migliorati ed approfonditi?

Note:

Allegati:

SEGNALAZIONE ERRORI

Pagina	Capitolo/Capoverso	Segnalazione errore

Azienda Ospedaliero Universitaria di Sassari

ISTRUZIONI PER LA SICUREZZA DEI DATI

Misure di sicurezza da applicare nei trattamenti di dati con strumenti elettronici

Documento	AOU-DPS-IST01/0
Edizione	31/03/2009

Premessa

L'**Autorità Garante della Privacy**, istituita nel 1996, si propone di tutelare il diritto alla privacy di tutti, sia che si tratti di persone fisiche ovvero di persone giuridiche, enti o associazioni. Vengono quindi focalizzati tutti i processi aziendali che interessano dati personali, entrando nel merito delle finalità e della liceità dei "trattamenti" che vengono effettuati.

In questo contesto l'Azienda Ospedaliero Universitaria di Sassari, in qualità di Titolare dei trattamenti dei dati necessari per l'espletamento della propria missione, dopo aver provveduto agli adempimenti previsti dalla Legge, intende sensibilizzare tutto il personale alle misure di sicurezza per la tutela dei dati e della Privacy .

Privacy e Sicurezza pur essendo distinte, sono intimamente legate tra loro.

Le misure di sicurezza sono il presupposto operativo e strumentale, certamente necessarie, ma non sufficienti per garantire quanto si prefigge il Garante.

Gli adempimenti richiesti dal Garante, le sanzioni e le pene, previste in caso di inadempienza, sono gli strumenti che la Legge usa per regolamentare ed intervenire.

Tuttavia, la vera tutela della Privacy non può che essere il risultato di un codice deontologico aziendale, fondato su valori etici e regole di comportamento che tutti devono conoscere, adottare e far rispettare.

Queste istruzioni sono destinate a tutto il personale Incaricato di effettuare trattamenti di dati con strumenti elettronici.

Indice del Contenuto

1 Introduzione

Il "Testo Unico sulla Privacy" (D. lgs.196/03: "Codice") entrato in vigore il primo gennaio 2004, riprende ed integra la normativa introdotta dalla Legge 675/96 e dal DPR.318/99, prevedendo l'obbligo di garantire la sicurezza, l'integrità e la disponibilità dei dati personali. Esso sancisce che:

"Chiunque ha diritto alla protezione dei dati personali che lo riguardano."

"I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità."

Si tratta di una regola di ordine generale in specie per i sistemi e i programmi che verranno d'ora in poi predisposti.

1.1 Definizioni

Riportiamo le definizioni del Codice:

a) **"trattamento"**, qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

b) **"dato personale"**, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

c) **"dati identificativi"**, i dati personali che permettono l'identificazione diretta dell'interessato;

d) **"dati sensibili"**, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

e) **"dati giudiziari"**, i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da *r*) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

f) **"titolare"**, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

g) **"responsabile"**, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h) **"Incaricati"**, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i) **"interessato",** la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

l) **"comunicazione",** il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli Incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

m) **"diffusione",** il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

n) **"dato anonimo",** il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

o) **"blocco",** la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

p) **"banca di dati",** qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

q) **"Garante",** l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

2 L'insieme delle misure di sicurezza

La sicurezza non deve essere intesa solo come protezione da eventi negativi, accidentali o intenzionali, ma anche come limitazione degli effetti causati dall'eventuale verificarsi di tali eventi di:

- **distruzione o perdita, anche accidentale, dei dati**: ossia si deve impedire che dati, informazioni e risorse siano resi irreperibili da persone, mediante processi non autorizzati, o da eventi accidentali. Nel mondo informatico si ricorre la concetto di ***disponibilità del dato,*** in tale ambito assume inoltre una particolare valenza il requisito della ***integrità del dato***, che deve essere quello originario o legittimamente modificato, in relazione alla relativa facilità di procedere fraudolentemente a modifiche senza lasciare indizi;

- **accesso non autorizzato ai dati**: nel mondo fisico è immediato pensare ad estranei, che nella notte si introducono in un'azienda per rubare dei dati o farne delle copie, piuttosto che a personale dell'azienda stessa che viola determinati archivi durante l'orario di lavoro. Nel mondo informatico si parla di ***confidenzialità*** o ***riservatezza,*** con ciò intendendosi che un determinato dato deve essere accessibile solo a chi è autorizzato: si dovrà quindi fare in modo che il personale non possa consultare files che non lo riguardano; che estranei non possano accedere abusivamente al sistema informativo; che durante la trasmissione di dati da un computer ad un altro, dei malintenzionati non intercettino i messaggi per violare le informazioni in essi contenuti. Correlato a tali aspetti vi è il requisito della ***autenticità*** dei dati, che concerne la garanzia e certificazione della loro provenienza;

- trattamento non consentito o non conforme alle finalità della raccolta.

L'insieme delle misure di sicurezza viene quindi concettualmente suddiviso in tre sottoinsiemi, distinguendo le ***misure***:

- ***organizzative***, che si sostanziano nella definizione di una serie di norme e procedure, miranti a regolamentare l'aspetto organizzativo del processo di sicurezza.

- ***fisiche***, il cui scopo è di proteggere le aree, le apparecchiature, i dati e le persone da eventi di natura accidentale (es. incendi) e da intrusioni, di personale non autorizzato o di terzi.

- ***logiche***, il cui campo di applicazione riguarda la protezione delle informazioni, con particolare riferimento a quelle gestite con i sistemi informativi (dati, applicazioni, sistemi e reti), sia in relazione al loro corretto utilizzo, che in relazione alla loro gestione e manutenzione nel tempo

2.1 Sensibilizzazione alla sicurezza

Tutto il personale deve tenere presente che le attività relative alla sicurezza non rappresentano un appesantimento del lavoro quotidiano, ma, una volta che entrano nel ciclo standard delle operazioni da compiere, contribuiscono a garantire tutti dal rischio di perdere, o comunque compromettere, parte del lavoro fatto.

La *sensibilizzazione* alle tematiche della sicurezza, ed a costanti comportamenti coerenti con le disposizioni date in merito, deve interessare tutto il personale dell'Azienda, ad ogni livello di responsabilità ed attività: ciò al fine di diffondere una cultura generalizzata

della sicurezza, che consenta tra l'altro di favorire la miglior efficacia ed efficienza delle misure prese, oltre che di sopperire ad eventuali mancanze delle stesse.

3 L'organizzazione per la sicurezza

L'Azienda Ospedaliero Universitaria di Sassari, nella consapevolezza che un sistema complesso quale la sicurezza può funzionare solo se i suoi meccanismi sono formalizzati e verificabili nonché posti in essere da personale adeguatamente formato e motivato, per l'applicazione e la gestione della normativa sulla privacy, ha provveduto ad adottare la seguente organizzazione per la sicurezza.

3.1 Titolare del trattamento

Ai sensi dell'art.4, lett. f) del Codice in materia di protezione dei dati personali, il Titolare dei trattamenti è l'Azienda Ospedaliero Universitaria di Sassari nella persona del Direttore Generale.

Il Titolare verificherà periodicamente che le istruzioni e le norme di legge in tema di privacy vengano correttamente applicate dai Responsabili.

3.2 Responsabili del trattamento

Il Titolare, nella persona del Direttore Generale dell'Azienda Ospedaliero Universitaria di Sassari, ha nominato Responsabili dei Trattamenti tutti i Dirigenti di Struttura i Dirigenti delle Unità Operative, i Dirigenti Amministrativi e i Dirigenti Responsabili dei Programmi ex art.5 comma 4 D.Lgs.517/99

3.3 Responsabile per la Sicurezza Informatica

Il Titolare, nella persona del Direttore Generale dell'Azienda Ospedaliero Universitaria, nominerà il Responsabile per la Sicurezza Informatica

Al Responsabile per la Sicurezza Informatica sono assegnati i compiti di:

- progettare, realizzare e mantenere in efficienza le misure di sicurezza, conformemente a quanto previsto dagli articoli 31 e 33 D. lgs. 196/2003;
- sovrintendere alle risorse del sistema informativo e di consentirne l'utilizzazione.

3.4 Incaricati

Il Titolare, nella persona del Direttore Generale dell'Azienda Ospedaliero Universitaria di Sassari, ha assegnato ai Responsabili la delega per la designazione degli Incaricati nelle strutture organizzative di pertinenza.

Ogni Incaricato ha, in ordine al trattamento, la responsabilità di eseguire correttamente le funzioni operative corrispondenti alle mansioni svolte nella struttura di pertinenza.

Le operazioni di trattamento di dati personali possono essere effettuate solo dagli Incaricati autorizzati dal Titolare o dai Responsabili.

Si tenga presente che tutto il personale sanitario, amministrativo e tecnico dell'Azienda che in qualche misura svolge attività che implicano il trattamento di dati personali, con particolare attenzione per quelli sensibili e giudiziari, dovrà essere designato quale Incaricato dei trattamenti di competenza.

4 Direttive ed istruzioni di carattere generale

Al fine di una corretta applicazione del D. Lgs. n. 196/2003, nonché di una adeguata tutela dei diritti degli interessati, i soggetti nominati Incaricati del trattamento dei dati personali dovranno osservare le seguenti direttive ed istruzioni generali.

Occorre ricordare che per trattamento di dati deve intendersi: "qualunque operazione o complesso di operazioni, svolte con o senza l'ausilio di strumenti elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati".

Sono dati personali tutte le informazioni che permettano l'identificazione del soggetto cui si riferiscono (es. dati anagrafici, recapiti telefonici, ecc.).

4.1 Modalità di trattamento e raccolta dei dati personali

L'Incaricato che riceve ed utilizza informazioni personali con modalità cartacee ed informatiche, raccolte presso gli stessi interessati o di altre fonti, deve sincerarsi che i dati siano:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati soli per scopi stabiliti, espliciti e legittimi;
- compatibili con quelli utilizzati in altre procedure e con gli scopi per i quali i dati sono stati raccolti;
- esatti e, se necessario, aggiornati;
- pertinenti e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- conservati in modo tale che l'identificazione dell'interessato sia possibile per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

A tal fine, il soggetto Incaricato dovrà:

- trattare tutti i dati personali di cui viene a conoscenza nell'ambito dello svolgimento delle proprie funzioni, in modo lecito e secondo correttezza;
- effettuare la raccolta, l'elaborazione, la registrazione, ecc. di dati personali esclusivamente per lo svolgimento delle proprie mansioni;
- accertarsi che gli atti e/o documenti nei quali sono contenuti i dati personali oggetto di trattamento dovranno essere custoditi presso gli archivi della propria struttura di riferimento e/o presso idonei ripiani del proprio ufficio, debitamente muniti di serratura;
- evitare che i documenti prelevati per il trattamento siano lasciati incustoditi, in modo da non consentirne l'accesso a persone non autorizzate;
- aggiornare trimestralmente/semestralmente tutte le banche dati cui ha accesso;

- mantenere assoluto riserbo sui dati personali di cui venga a conoscenza nell'esercizio delle proprie funzioni.

E' fatto assoluto divieto di comunicare, diffondere, utilizzare i dati personali provenienti dalle banche dati aziendali (dello studio, dell'associazione ecc.), in assenza di autorizzazione del Responsabile, che, in genere, è resa con l'attribuzione dell'incarico.

L'Incaricato deve verificare la sussistenza di tali requisiti in tutte le fasi del trattamento affidatogli, riportando al proprio Responsabile ogni situazione di criticità che dovesse rilevare.

Non è consentito all'Incaricato:

- utilizzare informazioni personali al di fuori di quelle necessarie per compiere le operazioni connesse alle sue specifiche mansioni;
- creare banche dati nuove senza espressa autorizzazione del titolare e/o del responsabile;
- conservare dati personali in archivi e banche dati al di fuori di quelle espressamente indicate nel Documento Programmatico sulla Sicurezza (DPS) o autorizzate dal Responsabile, considerato che eventuali nuovi trattamenti o trattamenti non censiti nel DPS dovranno immediatamente essere comunicati al Responsabile prima dell'avvio ;
- asportare supporti informatici o cartacei contenenti dati personali di terzi, senza la previa autorizzazione del Responsabile;
- comunicare o diffondere dati personali di cui gli Incaricati vengano a conoscenza nello svolgimento del proprio lavoro.

4.2 Particolari cautele per i dati personali "sensibili"

Gli Incaricati possono trovarsi, nell'esercizio delle propri funzioni, a trattare dati personali "sensibili".

Sono dati sensibili quei "dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale".

Costituendo tali dati il nucleo più intimo e personale della vita di ciascuno, il Codice prevede una disciplina particolarmente restrittiva e severa per il loro trattamento, prescrivendo anche ulteriori misure di sicurezza e modalità specifiche per la loro custodia.

Ne consegue che, in questi casi, l'Incaricato del trattamento di tale tipologia di dati, dovrà mantenere un comportamento adeguato alla cura ed al rispetto degli individui cui i dati si riferiscono, *adottando ogni precauzione che impedisca il rischio di perdita dei dati stessi o di cognizione (accesso) da parte di soggetti non autorizzati* ad esserne informati.

4.2.1 Dati sensibili in documenti cartacei

Nello specifico, a titolo esemplificativo e non esaustivo, le precauzioni che l'Incaricato sarà tenuto ad adottare nel caso in cui si trovasse a trattare dei dati sensibili, riprodotti su formato cartaceo, nello svolgimento delle proprie mansioni, sono le seguenti:

- gli atti ed i documenti che riproducono i dati sensibili dovranno essere conservati negli archivi del proprio ufficio o reparto, muniti di serratura;

- l'Incaricato potrà accedervi solo per motivi professionali ed esclusivamente durante l'orario di lavoro, nei limiti in cui ciò sia strettamente necessario per prelevare e riporre i documenti per lo svolgimento dei propri compiti;

- qualora dovesse assentarsi durante le sessioni di lavoro dalla propria postazione di lavoro, i documenti e gli atti dovranno essere custoditi negli armadi, scrivanie o cassetti, muniti di serratura, in modo da non consentire l'accesso a persone non autorizzate;

- in ogni caso, al termine delle operazioni di trattamento, gli atti ed i documenti dovranno essere riposti negli archivi, muniti di serratura, di cui al primo punto, da cui sono stati prelevati.

4.2.2 Dati sensibili in documenti informatici e/o elettronici

Per le cautele da adottare nel caso di trattamento di dati personali anche sensibili, effettuato mediante strumenti elettronici e/o informatici, si rinvia alle istruzioni dei capitoli seguenti relativi all'uso corretto degli strumenti informatici.

5 Modalità per un corretto utilizzo delle risorse informatiche aziendali

Premesso che l'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi ai principi di diligenza e correttezza che sono alla base di ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro, in coerenza con le previsioni di legge - artt. 2104 e 2105 c.c. - e contrattuali, si ritiene utile fornire ulteriori regole interne di condotta comune, dirette ad evitare comportamenti inconsapevoli e/o scorretti.

Nei casi in cui l'Azienda lo ritenga opportuno, tali regole potranno essere soggette a modifiche o integrazioni, tenuto conto anche dell'evoluzione normativa in materia e del progresso tecnologico, nonché degli sviluppi delle infrastrutture informatiche e produttive dell'Azienda, di cui tutti gli Incaricati verranno portati a conoscenza.

Le indicazioni che seguono si riferiscono a tutte le risorse informatiche di proprietà dell'Azienda Ospedaliero Universitaria di Sassari (nel seguito "l'Azienda") e si applicano a tutti i soggetti che le utilizzano (nel seguito "Utenti"), ivi incluso il personale esterno che accede alle risorse informative ed ai sistemi informatici dell'Azienda.

Per risorse informatiche si intendono i dati, le applicazioni e i sistemi (hardware e software di base).

L'Azienda emanerà periodicamente comunicazioni e direttive alle quali tutti gli Utenti sono tenuti a conformarsi.

5.1 Accesso alle risorse informatiche

Gli utenti hanno diritto ad accedere alle risorse informatiche aziendali per le quali sono stati espressamente autorizzati e ad utilizzarle esclusivamente per gli scopi inerenti le mansioni svolte.

Tali autorizzazioni sono strettamente personali e non cedibili.

Gli strumenti adottati dall'Azienda per l'accesso alle risorse informatiche (es. codici di accesso, user-id, ecc.) sono anch'essi di uso strettamente personale e, pertanto, l'Utente è tenuto a custodirli in modo appropriato.

Gli accessi alle banche dati informatizzate e/o ai dati personali oggetto di trattamento dovrà avvenire tramite l'elaboratore/gli elaboratori assegnati, anche temporaneamente, di cui l'Utente è personalmente responsabile durante il periodo in cui svolge la prestazione lavorativa, anche al di fuori del normale orario di lavoro; in particolare per quanto riguarda la corretta applicazione delle procedure e misure di sicurezza di seguito indicate.

Ai dati presenti nelle banche dati l'Utente è autorizzato a procedere per consultazioni, elaborazioni, aggiornamenti e cancellazioni secondo le sole esigenze richieste dalle sue mansioni professionali.

5.2 Utilizzo delle credenziali di autenticazione

Gli accessi tramite il computer agli archivi informatici sono protetti da una o più credenziali di autenticazione consistenti in uno o più user-id (identificativo utente) e da una o più password univoche, ovvero associate esclusivamente a ciascun Utente.

A ciascun Utente sono attribuiti, pertanto, una user-id nominativa ed una password di accesso ai sistemi informatici dell'Azienda. Saranno inoltre assegnate ulteriori user-id e password per l'accesso ai sistemi o a parte di essi a cui ciascun Utente è autorizzato ad accedere secondo i profili di autorizzazione riconosciuti.

Le password e lo/gli user-id verranno forniti per la prima volta dal Responsabile per la Sicurezza Informatica (o da un suo incaricato espressamente autorizzato).

Successivamente al primo utilizzo della password inizialmente comunicata l'Utente è tenuto a modificare la password fornita dal Responsabile per la Sicurezza Informatica (o da un suo incaricato espressamente autorizzato) e cambiarla con la frequenza e secondo le regole qui riportate e che verranno di volta in volta indicate.

Qualora per motivi di necessità ed urgenza sia indispensabile eseguire delle operazioni di trattamento di dati disponibili esclusivamente attraverso l'utilizzo delle credenziali di autenticazione e degli strumenti elettronici appartenenti ad altri Utenti (ad es Posta elettronica), ed in caso di loro prolungata assenza od impedimento, sarà comunicato all'Utente interessato una password provvisoria di accesso, previa autorizzazione del proprio "Responsabile.

Al termine delle operazioni effettuate l'Utente interessato dovrà comunicare al proprio "*Responsabile*" di aver terminato l'intervento indicando le operazioni da esso compiute.

Si fa presente che le password di accesso ai sistemi informatici sono di uso strettamente personale e devono essere mantenute riservate.

Non è permesso comunicarle ad alcuno.

Le password scelte dovranno avere una lunghezza non inferiore agli otto caratteri salvo che il sistema, l'applicazione o lo strumento elettronico non lo consentano e comunque, in questi ultimi casi, il numero dei caratteri dovrà essere uguale a quello massimo consentito.

Al fine di evitare accessi non autorizzati o non consentiti, rischi di intrusione nei sistemi informativi aziendali, di distruzione o perdita dei dati l'Utente è tenuto a non:

- comunicare la password per telefono o altro mezzo a soggetti che si presentano come colleghi, tecnici, supervisori ecc;
- digitare la password davanti ad altri (ad es. colleghi o estranei);
- scrivere la password su foglietti apposti al personal computer, lasciati sulla scrivania o dentro ad un cassetto;
- mantenere copia della/e password utilizzate, salvo che la copia sia conservata in un luogo accessibile al solo Utente.

Le tecniche più frequentemente impiegate per scoprire le password consistono in programmi che attingono ad esempio a dizionari o ad elenchi telefonici.

Nella misura in cui il sistema non lo imponga in maniera automatica è, quindi, raccomandabile non utilizzare una password facilmente deducibile da parte di terzi e quindi:

- non usare una password che:
  - sia un nome proprio di persona o derivante dallo userid (identico, inverso, con le lettere raddoppiate, ecc.);
  - sia composta di sole cifre o di una sola lettera o carattere anche ripetuto più volte, o ancora digitata attraverso l'uso della sola barra spaziatrice;
  - abbia riferimenti riconducibili a dati personali (indirizzo, telefono, codice fiscale, numero della patente,ecc.) o a dati dell'azienda (denominazione sociale, ufficio, struttura, ecc.) o alla data corrente;

- sia uguale alle ultime tre utilizzate o uguale alla precedente tranne che per un carattere.

- effettuare la sostituzione della password almeno ogni 30 giorni.

In generale, qualora si avesse anche solo il dubbio che sia venuta a conoscenza di altri è necessario:

- provvedere immediatamente alla modifica della password;
- segnalare al Responsabile per la Sicurezza Informatica la sospetta violazione.

5.3 Utilizzo del Personal Computer

All'Utente, nell'ambito del rapporto di lavoro, sono affidate in uso risorse informatiche dell'Azienda come personal computer, computer portatili, relativi programmi e/o applicazioni nonché informazioni in essi contenute. E' quindi necessario:

- custodirli in modo appropriato;
- utilizzarli per lo svolgimento delle attività lavorative, nell'ambito delle mansioni assegnate;
- non utilizzarli per scopi illeciti;
- mettere in atto tutti gli strumenti e le precauzioni necessarie al fine di evitare l'accesso alla risorsa da parte di soggetti non autorizzati, ogniqualvolta ci si allontana dal personal computer (ad es. procedere al blocco del computer oppure all'attivazione dello screen saver protetto da password).

Al fine di assicurare il corretto funzionamento delle applicazioni del personal computer (PC), nonché di evitare il grave pericolo di introdurre virus informatici all'interno della rete dell'Azienda, è opportuno che l'Utente:

- non modifichi, senza preventiva autorizzazione, le configurazioni impostate sul proprio PC;
- non rimuova o modifichi, senza preventiva autorizzazione, alcun dato o apparecchiatura aziendale;
- non installi sul proprio PC mezzi di comunicazione o altre periferiche proprie, senza preventiva autorizzazione (ad es.: modem, masterizzatori, etc..);
- non installi ed utilizzi software non autorizzati e comunque non di proprietà dell'Azienda;
- non utilizzi software ricevuto in uso al di fuori delle finalità lavorative, evitando, in particolare, di realizzare copie da cedere, a qualsiasi titolo, a terzi;
- non distribuisca (anche via e-mail) ed utilizzi software che possa danneggiare le risorse informatiche.

L'utilizzo di computer portatili richiede che gli Utenti applichino la dovuta attenzione all'attuazione delle procedure poste in essere dall'Azienda a garanzia della sicurezza informatica, specifiche per tali dotazioni, come ad esempio la necessità di collegarsi periodicamente alla rete aziendale per consentire l'aggiornamento delle configurazioni (aggiornamento patch e antivirus).

In particolare, il personale esterno non può connettersi alla rete aziendale con il proprio Personal Computer portatile se non previa esplicita autorizzazione dell'Amministratore del Sistema interessato.

In generale, è richiesta da parte dell'Utente l'adozione di cautele atte ad evitare qualunque tipo di azione il cui effetto consista nel provocare danni, anche permanenti, a sistemi informatici o telematici, nonché a dati, documenti e comunicazioni.

5.4 Utilizzo dei servizi aziendali di Rete

L'utilizzo delle risorse aziendali di rete (ad es. Posta elettronica, Internet) per motivi non attinenti allo svolgimento delle mansioni assegnate, provoca una distorsione dell'utilizzo delle risorse informatiche verso attività non di pertinenza dell'Azienda.

Alcuni atti, anche involontari, possono inoltre danneggiare seriamente l'Azienda.

Al fine di scongiurare tale pericolo è necessario che l'Utente eviti comportamenti come quelli qui di seguito richiamati a titolo indicativo.

5.4.1 Posta elettronica

Nel precisare che la Posta Elettronica è uno strumento di lavoro, si ritiene utile segnalare che l'Utente deve evitare di:

- utilizzare l'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, Forum o mailing-list non direttamente attinenti l'attività lavorative e le proprie mansioni, salvo diversa ed esplicita autorizzazione;
- effettuare ogni genere di comunicazione non afferente a ragioni di servizio, salvo diversa ed esplicita autorizzazione;
- simulare l'identità di un altro utente;
- inoltrare messaggi, comunicazioni o circolari non aventi contenuti di interesse aziendale utilizzando le liste di distribuzione;
- usare provider di posta elettronica diversi da quello aziendale, salvo esplicita autorizzazione del proprio Responsabile;
- prestare la massima attenzione nell'aprire allegati di posta elettronica "ambigui" (gli allegati possono, infatti, contenere virus o codici nascosti di natura dolosa che possono comportare la divulgazione di password o il danneggiamento di dati aziendali).

5.4.2 Internet

Per quel che riguarda le modalità di utilizzo della rete Internet, è opportuno segnalare che l'Utente deve evitare di:

- effettuare ogni genere di comunicazione non afferente a ragioni di servizio, salvo diversa ed esplicita autorizzazione;
- partecipare, per motivi non professionali a Forum, l'utilizzo di chat-line, di bacheche elettroniche e registrazioni in guest-book anche utilizzando pseudonimi (o nicknames);
- scaricare software gratuiti (freeware) e shareware prelevato da siti Internet, se non espressamente e preventivamente autorizzato;

- scaricare file multimediali per finalità non direttamente afferenti l'attività lavorativa, comunque sempre con esplicita autorizzazione del proprio Responsabile;

- scaricare documenti informatici di natura oltraggiosa o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione o appartenenza sindacale o politica.

5.4.3 Intranet

Le unità di rete aziendali sono aree di condivisione di informazioni strettamente professionali e non possono, in alcun modo, essere utilizzate per scopi diversi, pertanto gli Utenti non devono:

- modificare gli indirizzi IP assegnati ai propri PC;

- dislocare, nemmeno per brevi periodi, in queste unità, qualunque files che non sia legato all'attività lavorativa;

- trasferire su cartelle pubbliche dati non destinati alla diffusione, nonché dati d'interesse strategico aziendale (se non preventivamente autorizzati).

5.5 Gestione dei supporti fisici rimovibili

Per quanto concerne i supporti fisici rimovibili (es. floppy disk, dischi ZIP, CD,...), contenenti dati personali, devono essere attuate misure che garantiscano il salvataggio dei dati con frequenza almeno settimanale.

L'Azienda Ospedaliero Universitaria di Sassari prescrive inoltre agli Incaricati del trattamento quanto segue:

- i supporti devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono essere conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati o distrutti, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi;

- una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.

Segnalazioni e Suggerimenti

Questo documento dovrà evolversi per essere un utile strumento di lavoro, riflettendo i mutamenti dell'organizzazione e delle infrastrutture dell'AOU, e recependo le esigenze dei Responsabili e di tutti coloro che lo utilizzeranno.

Le Vostre segnalazioni e i Vostri suggerimenti sono molto importanti perché ciò avvenga.

Per farlo, potete inviare questo modulo debitamente compilato al Responsabile per la Sicurezza Informatica, che terrà in debito conto le Vostre osservazioni per migliorare le successive edizioni di questo documento.

Potete fotocopiare e compilare il modulo sottostante e quindi spedirlo all'indirizzo specificato, oppure inviare una e-mail con le stesse informazioni a sicurezza@aousassari.it

.....

Data _____

Da: _____

Unità _____

_____

_____

Tel _____

A: Responsabile Sicurezza Informatica
Azienda Ospedaliero Universitaria
Direzione Generale
Via M. Coppino, 26
07100 - Sassari

e-mail _____

COMMENTI E SUGGERIMENTI:

1) I contenuti del documento sono sufficientemente esaurienti in relazione alla finalità?

Si ☐ No ☐

2) Quali punti o argomenti ritenete debbano essere migliorati ed approfonditi?

Note:

Allegati:

SEGNALAZIONE ERRORI

Pagina	Capitolo/Capoverso	Segnalazione errore